# Consumer privacy: understanding the acceptance of consumer information collection

Beke, Franciscus Theodorus

# Consumer privacy: understanding the acceptance of consumer information collection

**Frank T. Beke**

Publisher: University of Groningen
Groningen, The Netherlands

Printer: Ipskamp Printing B. V.
Enschede, The Netherlands

ISBN: 978-94-034-0409-7 (book)
978-94-034-0410-3 (e-book)

rijksuniversiteit
groningen

# Consumer privacy: understanding the acceptance of consumer information collection

**Proefschrift**

ter verkrijging van de graad van doctor aan de
Rijksuniversiteit Groningen
op gezag van de
rector magnificus prof. dr. E. Sterken
en volgens besluit van het College voor Promoties.

De openbare verdediging zal plaatsvinden op

donderdag 8 februari 2018 om 14.30 uur

door

**Franciscus Theodorus Beke**

geboren op 1 november 1988
te Apeldoorn

**Promotores**
Prof. dr. P.C. Verhoef
Prof. dr. J.E. Wieringa

**Copromotor**
Dr. F. Eggers

**Beoordelingscommissie**
Prof. dr. J. Henseler
Prof. dr. K. van Ittersum
Prof. dr. C. Tucker

# Table of Contents

## Chapter 1.

# Introduction

We are living in the '*age of information'*. Every year 16.1 trillion gigabytes of data are recorded, and forecasts are that this will grow to 163 trillion gigabytes by 2025 (Reinsel, Gantz, and Rydning 2017). As firms began to realize that data could generate value for them and for their customers, they began collecting, storing and using more data (or information) about consumers than ever before. It allows firms to better understand their customers and provide products and services that better match consumers' needs and preferences. Customer Relationship Management, Customer Intelligence, and, more recently, one-to-one marketing have all emerged by virtue of collecting information (Rust and Huang 2014).

However, in this '*age of information'* privacy has become an important issue for firms (Wedel and Kannan 2016). In light of controversial revelations regarding privacy in general (e.g., Edward Snowden's disclosures about data collection and surveillance programs), concerns about privacy have risen worldwide. In the US, 92% of consumers worry about their online privacy (TRUSTe 2016), while globally 57% of consumers were more concerned about their privacy compared to last year (CIGI-Ipsos 2017). These concerns have triggered legislators in the US and the EU to develop privacy legislation aimed at providing consumers more control over '*their'* information. This could threaten firms, as these concerns deter consumers from accepting information collection. For example, a recent study by Pew Research shows that 60% of consumers have chosen to not install an app when the collection of information was considered excessive, while 43% have uninstalled an app after finding out about excessive information collection (Olmstead and Atkinson 2015). Even when consumers might not immediately abandon firms that neglect privacy, disregarding these concerns could result in (future) backlash. Given how important information has become to firms, it has become crucial to understand how privacy affects consumers, and more specifically, when and why consumers accept or reject the collection, storage, and use of information.

Over the past years, several examples have illustrated how firms tend to overlook or mismanage consumer privacy. For example, when US toy manufacturer Mattel introduced their new '*smart*' Barbie doll in 2015 they emphasized it could interact with children in a sensible manner. Instead of embracing the "*doll of the future*" however, consumers were highly upset because Mattel seemingly recorded and analyzed all conversations these children had with their doll (The Guardian 2015). Despite that consumers have indicated they accept information collection and use in exchange for benefits (PwC 2014), firms and consumers hold different opinions on whether the collection and use of information provides sufficient benefit to consumers (Deloitte 2014). As a prime example, Dutch bank ING was forced to cancel their plans to provide personalized discounts based on clients' payment information after it was publicly denounced (NU.nl 2014). On top of the critique that the benefits fail to compensate for the excessive information collection, storage, and use, consumers have complained about a lack of transparency and control (Eurobarometer 2011). For example, in 2013 consumers were highly upset that Nordstrom had been tracking the movement of individual customers in several of their stores without properly informing its customers or providing them with any possibility to prevent such tracking (Forbes 2013).

What is interesting about these and other examples is that firms seem to suffer from a lack of understanding on how consumers conceive their privacy practices. While firms continuously emphasize the benefits of collecting, storing, and using information, consumers increasingly focus on the (potential) negative consequences. Firms struggle with their privacy strategy, in particular with the role of transparency and control. The goal of this dissertation is to provide more insights into the role of privacy for firms and consumers. Specifically, we assess how privacy affects consumers, and how consumers take both the positive and negative consequences of the growing information collection into account. Thus, we aim to provide firms some much-needed guidance with regard to how they should manage consumers'

privacy by answering the following research question: *How do firms' privacy practices affect consumers?* Besides the collection, storage, and use of information, these privacy practices encompass transparency and control. In order to answer this question our first step is to conceptualize privacy. Hereafter we review the current literature on privacy in chapter 2, develop a measurement tool (PRICAL) to better understand consumers' acceptance of information collection in chapter 3, and assess how the influence of firms' privacy practices on the choices consumers make differs between industries in chapter 4.

## 1.1 Conceptualization of privacy

"*Privacy is a concept in disarray*" (Solove 2006, p.1) – In light of the rise of photography and growing circulation of newspapers at the beginning of the 20th century, legal scholars Warren and Brandeis (1890) stressed the importance of privacy as "*the right to be let alone*". Besides preventing other from intruding your personal sphere, such as your house, they stated every individual should be protected against improper publications. While the initial focus was on others being physically present in your personal sphere (physical privacy), the growing collection, storage, and use of personal information[1] has shifted our attention to informational privacy (Goodwin 1991; Mason 1986; Rust, Kannan, and Peng 2002). For informational privacy intrusion relates more to others monitoring and recording your behavior, and thus to the collection and storage of information, without necessarily being physically present. Meanwhile, protection from improper publications relates to how information is used. The growing importance of consumer information directs the focus throughout this dissertation to informational privacy of consumers, to which we will simply refer as '*privacy'*.

There has been much discussion on how privacy should be defined. Some scholars have suggested that as privacy is context-specific, it cannot be properly defined (Martin and Murphy 2017; Pavlou 2011; Smith, Dinev, and Xu 2011). This literature stream has proposed

[1] In line with recent legislation, we consider personal information to be all information that can be attributed to one individual (General Data Protection Regulation (EU) 2018).

to focus on harmful practices with information instead (Prosser 1960; Solove 2006), whereby context-specific norms determine whether activities are harmful and thus violate privacy (Nissenbaum 2004). Despite these suggestions, we follow the juridical standpoint that privacy is matter of autonomy and control over the collection, storage, and use of information (Altman 1975; Malhotra, Kim, and Agarwal 2004; Petronio 1991; Smith, Milberg, and Burke 1996; Stone et al. 1983; Westin 1967). Recent privacy laws and guidelines in the US and the EU have also adopted this standpoint on privacy, as they aim to let consumers decide for themselves what happens with '*their*' information. This implies that while in the context of privacy the collection, storage, and use of information all matter, privacy is only violated when information is collected, stored, or used against the consumer's will.

For consumers '*effective'* control depends on being aware of and having the ability to influence the collection, storage, and use of information (Caudill and Murphy 2000; Foxman and Kilcoyne 1993; Goodwin 1991). Therefore, in the context of firms and consumers we define privacy as *the extent to which a consumer is aware of and has the ability to control the collection, storage, and use of personal information by a firm*. Thus, in the context of privacy the collection, storage, and use of information all matter. However, if firms want to respect consumers' privacy they should explain what information they collect, how they store the information, and for which purposes they will use the information (transparency). Moreover, firms should allow consumers to prevent them from collecting information, to force them to discard information, and to prohibit them from using their information (control).

Across a wide range of disciplines, ranging from social psychology to information systems and, more recently, marketing, there has been a debate about what privacy is and what privacy is not (Smith, Dinev, and Xu 2011; Spärck Jones 2003). Because privacy is contingent on control, knowingly disclosing information or accepting information collection is not a violation or deterioration of privacy. This contrasts with the economic view on

privacy (Posner 1978, 1981; Rust, Kannan, and Peng 2002), which considers privacy as concealing or withholding information, and thus as secrecy or confidentiality. Although related, privacy is also not the equivalent of security, as that implies that (unknown) outsiders illegally—that is, without proper authorization—intercept or access information (Belanger, Hiller, and Smith 2002; Hoffman, Novak, and Peralta 1999; Martin, Borah, and Palmatier 2017). Given that when security fails, information is collected, stored, or used without consumers knowingly consenting, security can be considered as one requirement for ensuring privacy and will be treated as such.

## 1.2 Outline of the dissertation

The general aim of this dissertation is to provide more insights into the role of privacy for firms and consumers. More specifically, Table 1-1 shows an overview of the contribution(s) per chapter. In chapter two we provide an outline of the current empirical findings on the influence of privacy (concern) on consumers, and we discuss the theoretical frameworks that have been used to understand when and why consumers accept information collection. More specifically, we highlight when consumers withhold (or falsify) information, reject information collection, or otherwise behave differently owing to a firm's privacy practices. In addition, we summarize how consumers are affected when confronted with the storage and use of personal information, through marketing communication or location-based services. Besides these main effects we briefly discuss whether these findings differ between firms, consumers, and environments. By structuring the current knowledge we are able to identify research gaps, for which we formulate research propositions aimed at providing direction for future research regarding the role of privacy in marketing. All in all, this chapter provides an overview on what is currently known about privacy in light of customer-firm relationships, and highlights areas that are in need for future research.

**Table 1-1.** Contribution(s) of dissertation

| Contribution(s) | Chapter 2 | Chapter 3 | Chapter 4 |
|---|---|---|---|
| Outline of empirical findings on the influence of a firm's privacy practices on consumers | ✓ | | |
| Direction for future research on the influence of a firm's privacy practices on consumers | ✓ | | |
| Conceptualization and operationalization of the privacy calculus | | ✓ | |
| Enhanced understanding on the acceptance of information collection, storage, and use | | ✓ | |
| Insights on the (relative) influence of a firm's privacy practices on a consumer's acceptance of information collection | | | ✓ |
| Understanding on whether the influence of a firm's privacy practices differs between industries | | | ✓ |

As depicted in Figure 1-1, we look at privacy from a consumer perspective in chapter three, as we try to understand why consumers accept or reject that firms collect information about them. Rather than focusing on privacy concern, which has not always been consistent with how consumers behave (*privacy paradox*), we suggest looking beyond the negative consequences and also taking the positive consequences into account. We conceptualize consumers' entire privacy trade off (*privacy calculus*) by identifying the (perceived) consequences of the collection, storage, and use of information that matter to consumers. Besides the perceived valence of these consequences we follow perceived risk theory by

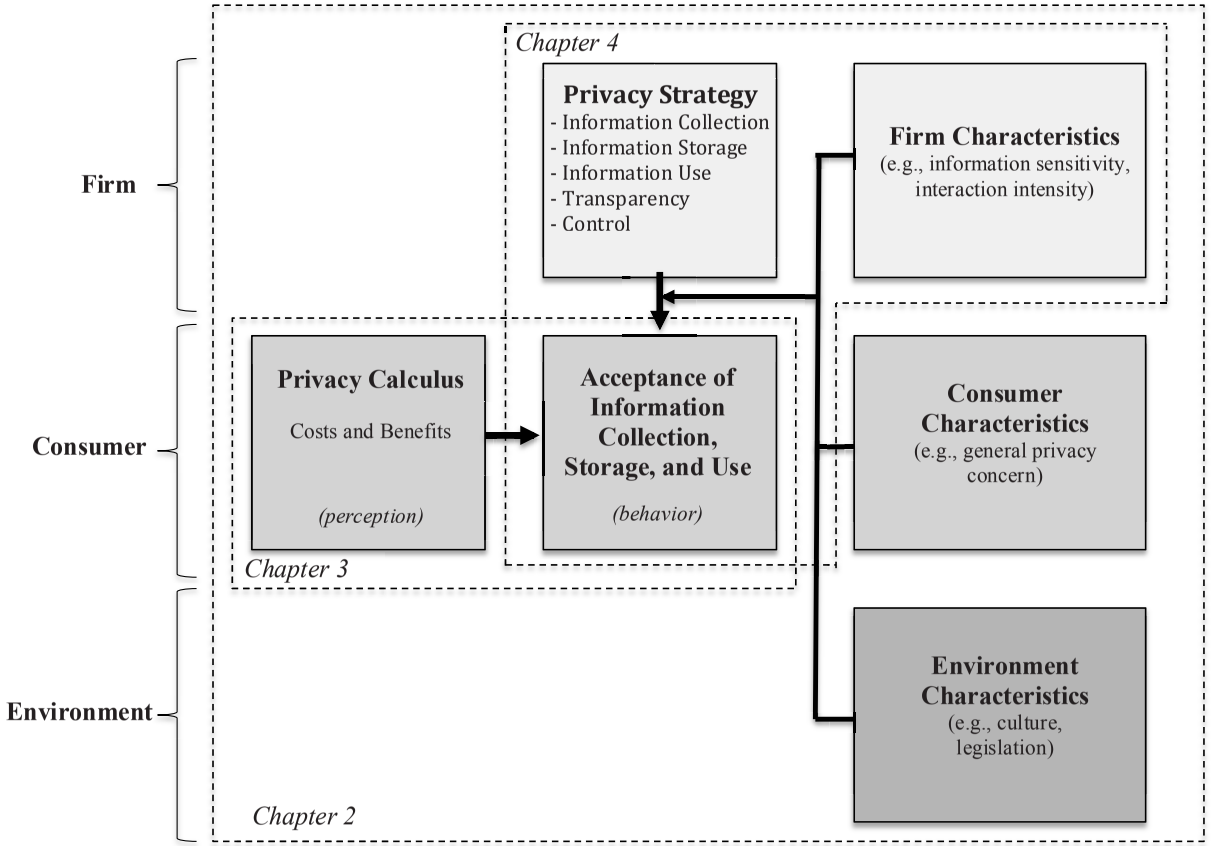



**Figure 1-1.** Outline of dissertation

accounting for the perceived probability of these consequences. On the basis of this conceptualization, we develop the PRICAL index, which measures consumers' privacy calculus using formative items. Following a qualitative phase to generate an initial list of items, we empirically purify this list and confirm the validity of the remaining items (Study 1) and the index as a whole (Study 2 and 3). On top of being embedded in theory, the privacy calculus construct and the PRICAL index better explain behavioral intentions (Study 2) and actual behavior (Study 3) than currently used constructs (e.g., privacy concern, trust). In sum, by conceptualizing the privacy calculus and developing the PRICAL index this chapter provides a better understanding of when and why consumers accept the collection, storage, and use of information.

In contrast to the third chapter, we discuss privacy more from a firm (strategy) perspective in chapter four. As the aforementioned examples illustrate firms have difficulties managing consumers' privacy. Therefore, we suggest that the growing attention for privacy represents an opportunity for firms that optimize their privacy strategy. What complicates matters is that besides looking at outcomes (distributive fairness, i.e., information collection, storage, use) consumers also take the way these outcomes come about (procedural fairness, i.e., transparency, control) into account. We use a choice-based conjoint experiment to show that when consumers have to decide upon adopting a product or service that is contingent on information collection all these privacy practices are of consequence, while comparing industries based on interaction intensity shows less variation. More importantly, the influence of a firm's privacy strategy depends on the status quo in their industry. Given our focus on elements of firms' privacy strategy that are under managerial control this chapter provides managerial recommendations with regard to which privacy strategies consumers are (less) inclined to accept across industries.

In chapter five we provide an overview of our findings regarding the role of privacy. We reiterate both our theoretical and practical implications, and formulate recommendations to managers that aim to improve their privacy strategy. Furthermore, we highlight the limitations of our research, and provide direction for future research. In summary, we contribute by providing a better understanding on how privacy affects firms and consumers.

**Table 1-2.** Overview of dissertation

| | **Chapter 2** | **Chapter 3** | **Chapter 4** |
|---|---|---|---|
| Contribution(s) | Outline of empirical findings on the influence of privacy practices on consumers | Conceptualization and operationalization of privacy calculus | Relative influence of privacy practices on consumers across different industries |
| Theoretical foundation | Various | Privacy Calculus<br>Perceived Risk Theory | Privacy Calculus<br>Social Exchange Theory |
| Methodology | Conceptual, Literature Review | Empirical, Index development (surveys) | Empirical, Choice-based conjoint experiment |
| Data sources | N/A | Research panel(s) (N = 300, N = 368)<br>Insurance firm (N = 700) | Research panel (N = 841) |

# Chapter 2

# Consumer Informational Privacy: Current Knowledge and Research Directions

**Abstract**

In the current '*age of information*' and '*big data*', consumer informational privacy has become an important issue in marketing. Besides being worried about the growing collection, storage, and use of personal information, consumers are anxious about a lack of transparency or control over '*their*' personal information. Despite these growing concerns, understanding of how firms' privacy practices affect consumers remains limited. We review the relevant literature on consumer privacy from a marketing perspective and summarize current knowledge about how information collection, information storage, information use, transparency, and control influence consumers' behavior. In addition, we summarize to what extent the influence of firms' privacy practices differs between firms, consumers, and environments. On the basis of this knowledge, we formulate research propositions aimed at providing direction for future research regarding the role of consumer privacy in marketing.

This paper is based on Beke, Frank T., Felix Eggers, Peter C. Verhoef (2017), "Consumers Informational Privacy: Current Knowledge and Research Directions", working paper

## 2.1 Introduction

Collecting information about consumers is imperative for marketers (Boulding et al. 2005; Rust and Huang 2014). Besides fostering better understanding of consumers' needs, it enables marketers to develop and maintain long-term relationships with their customers (Verhoef, Kooge, and Walk 2016). More recently, collecting and using personal information has allowed firms to adapt their marketing mix to specific individuals at specific locations at a specific moment in time (Chung, Wedel, and Rust 2016; Luo et al. 2014). The growing digitalization and recent rise of '*smart*' devices that create and collect detailed information about their users has spurred even more growth of information.

However, the expansion of information collection and use has resulted in a worldwide surge of privacy concern. These concerns could deter consumers from accepting information collection, which matters even more in times in which privacy legislation and technological innovations—such as cookie blockers and privacy-protective browsers—provide consumers more control over their privacy. Even when consumers might not immediately abandon firms that neglect privacy it could result in bad publicity and a loss of trust in case consumers find out about the collection, storage, and use of information afterwards. For example, when consumers became aware Samsung was recording all interactions with their '*smart*' TVs criticism went as far as accusing Samsung of spying on their customers (Forbes 2015).

Despite the growing importance of privacy, the understanding of how firms' privacy practices affect consumers and their relationships with firms is in its infancy. As privacy is an interdisciplinary topic, the knowledge about privacy and information disclosure is dispersed across scientific domains, ranging from social psychology to information systems and public policy. Within marketing, privacy has mainly been studied in the direct or interactive marketing literature (Culnan 1995; Milne and Boza 1999; Milne and Gordon 1993; Nowak and Phelps 1995; Phelps, Nowak, and Ferrell 2000; Schoenbachler and Gordon 2002), as part

of service quality (Parasuraman, Zeithaml, and Malhotra 2005; Wolfinbarger and Gilly 2003), or, more recently, in the literature on online advertising (Bleier and Eisenbeiss 2015a; Van Doorn and Hoekstra 2013; Goldfarb and Tucker 2011b; Schumann, Von Wangenheim, and Groene 2014; Tucker 2014). Although Peltier, Milne, and Phelps (2009) and Martin and Murphy (2017) have provided a global overview on the role of privacy within marketing, due to their broad focus the specific understanding of how firms' privacy practices affect consumers remains limited. While Lanier and Saini (2008) address part of this void by discussing (some) firm-related privacy issues, we believe a more structured overview focused on the influence of firms' privacy practices on consumers remains necessary. Specifically, firms need a fuller understanding of when and why consumers are (un)willing to disclose information and how a firm's privacy strategy affects the relationship with their customers, even to the point consumers might consider switching to a competing firm.

Our first objective is therefore to synthesize current knowledge about privacy and information disclosure by outlining the main empirical findings regarding the influence of firms' privacy practices on consumers, their privacy concerns, and the exchange of information.[2] Organizing the current knowledge based on the way firms handle the information (collection, storage, use) and privacy (transparency, control) of consumers allows for a structured, more detailed account on the influence of privacy on consumers. In addition, we discuss how the influence of these privacy practices on consumers differs between firms, consumers, and contexts. Second, drawing on our structured overview of the current knowledge we identify areas in need of insights, for which we formulate research propositions to stimulate future research. Before summarizing the current knowledge however we reiterate our conceptualization of consumer informational privacy, and then derive a conceptual framework, which guides the subsequent sections.

[2] Given our focus on empirical findings we exclude papers describing economic models (for an overview, see Acquisti, Taylor, and Wagman 2016) or those exploring the influence of public policy (Adjerid et al. 2016; Miller and Tucker 2009).

## 2.2 Conceptual framework

As discussed in chapter 1 our focus is on (consumer) informational privacy, which in line with the juridical standpoint is a matter of autonomy and control (Petronio 1991; Stone et al. 1983; Westin 1967). Therefore, in the context of firms and consumers we define informational privacy as *the extent to which a consumer is aware of and has the ability to control the collection, storage, and use of personal information by a firm*. In line with recent legislation, this implies that privacy is contingent on transparency and control, while personal information refers to all information that relates to an individual consumer (General Data Protection Regulation (EU) 2018).

Figure 2-1 presents our conceptual framework, which guides our discussion of the literature. We will discuss how firms' privacy practices, which encompasses the way firms handle the information and privacy of consumers, affects consumers' attitudes, intentions or behavior. Specifically, we discern five privacy practices that matter to consumers: information collection, information storage, information use, transparency, and (consumer) control. Understanding when consumers withhold (or falsify) information, reject information collection, or even refuse to interact or transact with a particular firm owing to its privacy practices has become crucial for managers. Moreover, firms need to know how consumers are affected when confronted with the storage and use of personal information, through marketing communication or location-based services.

Consumers' attitudes or perceptions with regard to privacy (e.g., privacy concern) often mediate the effect of firms' privacy practices on consumers' intentions or behavior. Therefore, many studies have used these attitudes or perceptions either as a proxy for firms' privacy practices (predictor) or as surrogates for consumer behavior (outcome). What complicates matters is that the influence of firms' privacy practices on consumers could differ between firms, consumers, and environments. For example, consumers accept the collection

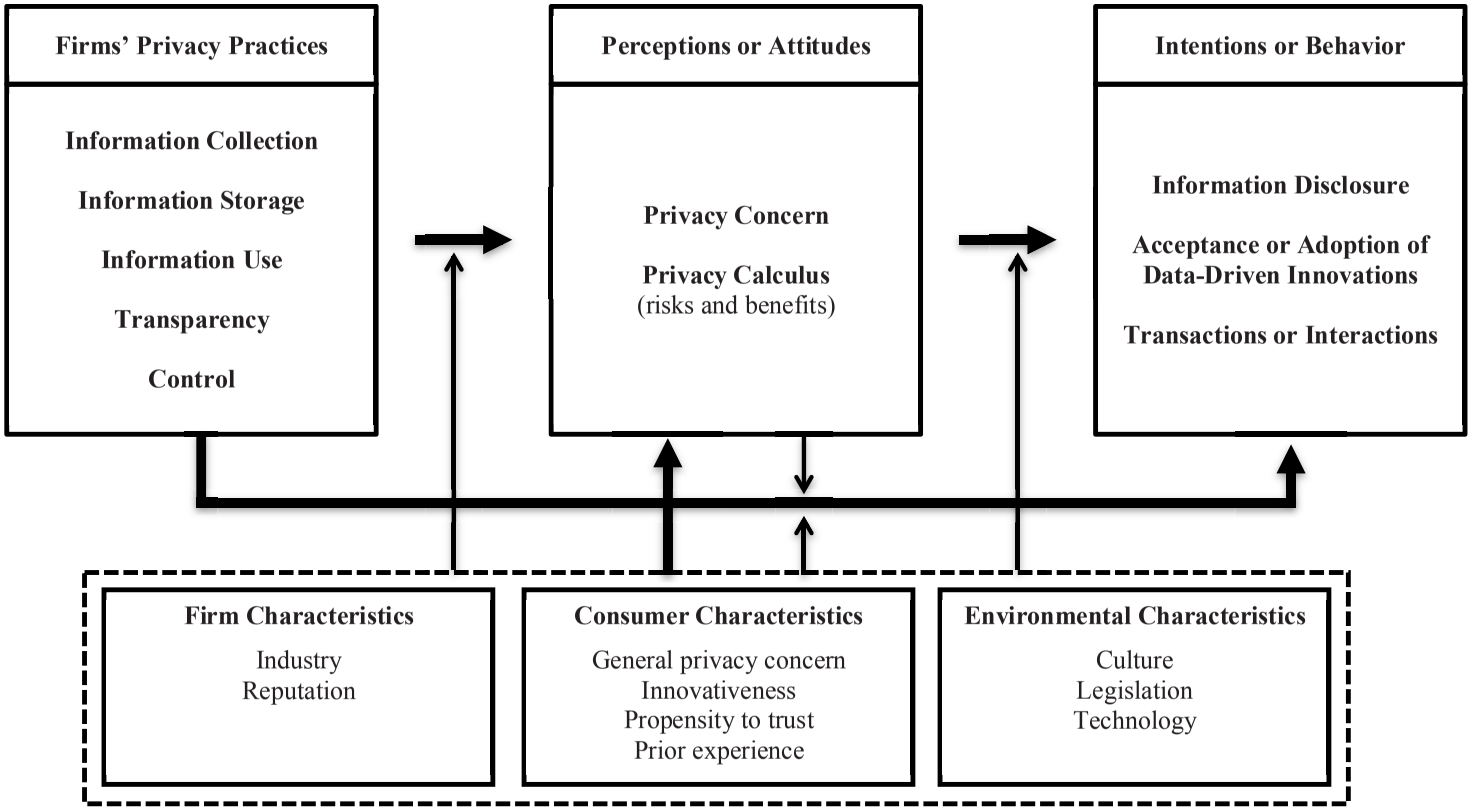



**Figure 2-1**. Conceptual framework

of medical information more easily when done by healthcare providers (firms), when being in perfect medical condition (consumers), or when privacy is regulated (environment).

To explain the influence of firms' privacy practices on consumer behavior, most studies have focused on the construct of privacy concern. Although conceptualized and operationalized in various ways, privacy concern always captures consumer's perceptions (or attitudes) of how the collection, storage, and use of personal information, or (lack of) transparency or control, negatively affect them (Malhotra, Kim, and Agarwal 2004; Smith, Milberg, and Burke 1996). Whereas the collection, storage, and use of personal information matter due to the negative consequences consumers may endure (distributive fairness), social contract theory suggests that transparency and control matter as consumers also take the procedures and interpersonal treatment (procedural fairness) into account (Donaldson and Dunfee 1994). The importance of transparency and control is also established in reactance theory, which proposes people resist from being restricted in their choices (Brehm 1966). In the context of privacy this implies that consumers will respond positively (negatively) when they believe firms are (not) transparent and provide (no) control over the collection, storage, and use of personal information (Culnan and Bies 2003; Son and Kim 2008). Besides privacy concern, Table 2-1 provides an overview of related constructs scholars have used to capture consumers' worries or uneasiness (attitudes and perceptions), such as privacy risk (Featherman, Miyazaki, and Sprott 2010), perceived privacy (Dinev et al. 2013), information sensitivity (Mothersbaugh et al. 2012), intrusiveness (Burgoon et al. 1989; Li, Edwards, and Lee 2002), and vulnerability (Martin, Borah, and Palmatier 2017).

Prior work has applied various theoretical frameworks to explain why consumers disclose information despite being concerned. Consumers' ability to protect their own privacy (protection motivation theory) (Rogers 1975; Youn 2009), or their trust in specific firms (Morgan and Hunt 1994; Wirtz and Lwin 2009) might diminish consumers' concerns in a

**Table 2-1.** Privacy concern and related constructs

| Construct | Definition | Source |
|---|---|---|
| Privacy concern | A consumer's worries or uneasiness with regard to the collection, storage, and use of personal information, or (a lack of) transparency and control | Smith et al. (1996); Malhotra et al. (2004) |
| Privacy risk | Subjective assessment of potential losses of confidential personally identifying information, including potential misuse | Featherman et al. (2010) |
| Perceived privacy | An individual's self-assessed state in which external agents have limited access to information about him or her | Dinev et al. (2013) |
| Information sensitivity | The potential loss or risk for consumers when information is disclosed | Mothersbaugh et al. (2012) |
| Intrusiveness | The extent to which an individual perceives unsolicited invasion in his or her personal sphere | Burgoon et al. (1989) |
| Vulnerability | Perception of susceptibility to harm owing to unwanted use of personal data | Martin et al. (2017) |

specific context. More recently the rationale that consumers look beyond the negative outcomes (concerns), and also take the positive outcomes of the collection, storage, and use of personal information into account, has taken root. Being closely related to social exchange theory (Homans 1958; Premazzi et al. 2010) and expectancy theory (Hann et al. 2007; Vroom 1964), the privacy calculus suggests that consumers determine for themselves whether they

regard the consequences of the collection, storage, and use of personal information to be beneficial (providing benefits) or detrimental (incurring costs or risks) in a specific situation (Culnan and Armstrong 1999; Dinev and Hart 2006; Laufer and Wolfe 1977). These consequences can be tangible (e.g., monetary discount) or intangible (e.g., uncomfortable feeling), and have been explained using more generic theoretical frameworks have also been applied, such as the theory of reasoned action (Fishbein and Ajzen 1975) or the technology acceptance model (Davis 1989). The privacy calculus is however considered as the "*most useful framework*" to understand the acceptance of information collection (Culnan and Bies 2003, p.326). Since the privacy calculus can accommodate most theoretical frameworks it has seen many explicit or implicit applications (e.g., Dinev and Hart 2006; Mothersbaugh et al. 2012; Premazzi et al. 2010; Xie, Teo, and Wan 2006), and will serve as foundation for this review as well.

### *2.2.1 The privacy calculus and the privacy paradox*

Despite the growing prominence of the privacy calculus, in some situations consumers' privacy attitudes or perceptions are inconsistent with their actual privacy-related behavior—a discrepancy that has been termed the '*privacy paradox*' (Berendt, Günther, and Spiekermann 2005; Norberg, Horne, and Horne 2007). Researchers have offered various explanations for its existence (Acquisti, Brandimarte, and Loewenstein 2015; Dinev, McConnell, and Smith 2015). Besides that some part of consumer behavior is inherently inconsistent or suffers from bounded rationality (Ariely 2009), consumers' privacy concerns are seldom triggered. Especially in low-involvement situations, such as when consumers search online or use their mobile phone, the influence of biases and heuristics can be strong (Chaiken 1980; Petty and Cacioppo 1986). In other instances, consumers are unable to respond because they are unaware that information is being collected or used (Acquisti and Grossklags 2005a), lack the ability to control firms' privacy practices (Turow et al. 2009), or have no suitable alternatives.

Apart from irrational behavior or situations in which consumers are unaware or unable to exert control, the privacy paradox has also been a measurement issue. Given that consumers' privacy preferences are strongly influenced by situational or contextual characteristics (Nissenbaum 2004), when and for which context privacy concern is measured matters—that is, privacy concern with regard to a specific technology (e.g., the Internet), a specific firm (e.g., Google), or a specific situation (e.g., when searching for a product). Moreover, as the benefits are typically measured using very generic measures (e.g., Xu et al. 2009, 2011), whether all benefits have been accounted for remains uncertain. In addition, the consequences (benefits and costs) of the collection, storage, and use of information are not always immediate and definite (Brandimarte, Acquisti, and Loewenstein 2013), which suggests that the perceived probability of consequences should be taken into account (Risk Theory, Bauer 1960; Conchar et al. 2004). So we conclude that consumers' acceptance of the collection, storage, and use of personal information is best explained by their context-specific perception of the benefits and costs, taking into account transparency, control, and the uncertainty of these benefits and costs.

## 2.3 Information collection

### *2.3.1 Amount and type of information*

Nowadays firms collect more information about their consumers than ever before. In general holds that the more information firms demand, the less willing consumers are inclined to provide (Hui, Teo, and Lee 2007). Consumers feel more vulnerable when firms have access to more information (more risk), which leads them to provide erroneous information, initiate negative word of mouth, or even switch firms (Martin, Borah, and Palmatier 2017).

Firms collect information about consumers' online behavior (e.g., click-stream data, social media), offline behavior (e.g., transaction records, location data), and information needed for interactions or transactions (e.g., contact information, financial state). Consumers

are affected by '*what'* firms want to collect, as they rather disclose lifestyle or purchasing habits than financial or medical information (Lwin, Wirtz, and Williams 2007; Mothersbaugh et al. 2012; Phelps, Nowak, and Ferrell 2000; Premazzi et al. 2010). Consumers disclose less information when they consider information to be sensitive (Acquisti, John, and Loewenstein 2012; Brandimarte, Acquisti, and Loewenstein 2012; John, Acquisti, and Loewenstein 2011), with sensitivity increasing when the potential for loss (or risk) becomes greater (Mothersbaugh et al. 2012). More recent work has shown that different types of information (e.g., financial information, medical information) result in different types of losses (e.g., monetary loss, social loss) (Milne et al. 2017). Therefore, consumers may consider information as sensitive for various reasons. For example, disclosing embarrassing information (e.g., sexual fantasies) might result in a loss of face, while disclosing identifiable information (e.g., name) might result in a loss of anonymity (White 2004). Understanding which types of information result in which types of losses, and which loss is considered most troublesome, would help firms mitigate consumers' concerns.

### *2.3.2 Information collection method*

Besides '*what'* firms collect also '*how'* they collect information matters. Digitalization has radically changed the way firms collect information about consumers. Rather than collecting information in person firms nowadays primarily gather information via computers or other information systems. Consumers respond positively when information is collected by computers rather than humans, such as employees (Schwaig et al. 2013), as without humans involved consumers have a sense of anonymity (Tourangeau and Yan 2007). Another consequence of digitalization has been that consumers have to decide whether they accept that firms collect information about them automatically rather than actively disclosing information themselves, for example via forms. This shift makes the collection of information less visible, which could amplify the privacy paradox. Moreover, it has started to give consumers the

feeling information is being collected behind their backs (Acquisti and Grossklags 2005a), which could result in a backlash when consumers eventually learn that firms have collected their information without notifying them—that is, without transparency (see below).

A recent development with regard to '*how'* firms collect information has been that besides active and passive information collection firms have increasingly began to rely on making inferences about consumers. For example, firms derive consumers' product preferences based on prior purchases. Despite that most (data-driven) firms make these inferences, and that such information could generate value for firms and their customers, consumers have indicated opposition to inferred information (Culnan 1993). While the underlying reason(s) are not clear, one issue could be that because inferences are not factual information, consumers fear they might be inaccurate. Moreover, making inferences might indicate that firms are hesitant to ask consumers for this information directly, which suggests the information is either sensitive or potentially negative in its effects on consumers. Finally, consumers might oppose inferences because they lack any control over when and which inferences firms make.

**Proposition 1**: Consumers oppose firms generating information by making inferences because (1) inferences might be inaccurate, (2) inferences might affect consumers negatively, or (3) they consider making inferences to be unfair.

#### *2.3.3 Online vs. Offline behavior*

Besides that firms are able to closely monitor how consumers behave online, more recently mobile phones and other '*smart*' devices provide firms with access to information regarding consumers' offline behavior. Consumers worry more about their offline identity ("*real life*") than about their digital identity ("*virtual life*") (Acquisti and Grossklags 2005b). Therefore, consumers are expected to be reluctant towards firms monitoring how they behave in stores (e.g., via RFID), on the road (e.g., via GPS), or in their own home (e.g., via a smart TV

connected to the Internet). If firms want to deal with this reluctance they need more insights as to when and why this is the case.

Contextual integrity and the influence of context-specific norms (Nissenbaum 2004) provide a reasonable explanation for consumers' reluctance towards allowing firms to monitor their offline behavior. The norm (and law) in most countries is that consumers should be able to behave without others continuously watching over their shoulder, especially in consumers' personal sphere, such as their home. Without doing something illegal, consumers might not feel comfortable when firms monitor and record socially sensitive behavior, such as going to the bathroom. Therefore, when firms have announced they would start monitoring consumers' offline behavior, such as Google via their '*smart*' home device, consumers immediately expressed their concerns (Huffington Post 2017).

**Proposition 2**: Consumers are more reluctant to let firms collect information about their offline behavior than online behavior because consumers expect they can behave freely (i.e., without firms monitoring them) in their personal sphere, such as at home.

#### *2.3.4 Monetary compensation and other persuasion methods*

Without changing the '*what'* and the '*how'* of information collection, and in line with the privacy calculus, firms have convinced consumers to disclose information by compensating them with additional benefits or monetary incentives. Some of these benefits are linked to information use, such as the ability to personalize products or services (see below). Also unrelated incentives, such as discount vouchers or access to free content, can persuade consumers to disclose information (Hui, Teo, and Lee 2007; Premazzi et al. 2010) or let firms track their behavior (Acquisti, John, and Loewenstein 2013; Derikx, de Reuver, and Kroesen 2016). Preliminary evidence suggests that monetary compensation gives consumers the feeling that they are '*selling*' their information, so they expect less control and allow firms to use the information any way they like (Gabisch and Milne 2014). The attractiveness of

monetary benefits is also reflected in consumers' adoption of loyalty programs. Multiple studies have shown that although consumers are worried about their privacy, discounts and other monetary benefits convince them to adopt loyalty programs nonetheless (Demoulin and Zidda 2009; Dorotic, Bijmolt, and Verhoef 2012; Leenheer et al. 2007).

However, providing monetary compensation becomes less effective when the risks of sharing information become higher—an effect that depends on both the amount and the type of information (see above). Moreover, preliminary evidence suggests that insufficient monetary compensation could arouse consumers' privacy concern (Andrade, Kaltcheva, and Weitz 2002), and that monetary compensation could deter consumers from disclosing information when the information is incongruent with the products and services of the firm (Li, Sarathy, and Xu 2010). Therefore, firms have to be cautious when offering a monetary compensation. Future research should clarify the boundary conditions for monetary compensation, and should assess to what extent the effectiveness of monetary compensation differs between firms and consumers.

**Proposition 3**: Monetary compensation becomes less effective (or even detrimental) for increasing willingness to disclose information when firms want to collect (1) more information, (2) more sensitive information, or (3) incongruent information.

Besides monetary compensation, there are other ways for firms to '*persuade*' consumers to disclose information. For example, when computers disclose information first consumers reciprocate by also disclosing information, (Moon 2000; Zimmer et al. 2010). Moreover, consumers disclose more information in unprofessional environments in which privacy is triggered less (John, Acquisti, and Loewenstein 2011), and driven by comparative judgment they disclose more when they believe other consumers have disclosed similar information (Acquisti, John, and Loewenstein 2012). Besides these methods, we propose that firms could also '*persuade*' consumers to accept information collection by collecting information in small

steps. Humans do not always take in gradually increasing risks (Slovic 2000), which suggests that firms could benefit from collecting less or less sensitive information from consumers first before requesting more or more sensitive information. Although in surveys respondents provide more answers when intrusive questions are asked first (Acquisti, John, and Loewenstein 2012), firms might be better of gradually increasing the amount or the sensitivity of information requested, as otherwise they might scare off consumers when they immediately want to collect sensitive information.

**Proposition 4**: Consumers are (1) willing to disclose more information when firms collect (additional) information in small steps, and (2) more willing to disclose sensitive information when they have previously disclosed less sensitive information.

## 2.4 Information storage

### *2.4.1 Security breach*

After collecting information about consumers, firms have to decide how and where to store the information. One thing that matters to consumers is that unknown outsiders cannot gain unauthorized access to their personal information (Smith, Milberg, and Burke 1996). Therefore, information storage relates closely to security. Over the past years, security breaches have become more common. In 2016, US firms and government agencies suffered over 1,000 security breaches, which were 40% more security breaches than the year before (Bloomberg 2016). These security breaches have shown to negatively affect stock prices (Acquisti, Friedman, and Telang 2006; Cavusoglu, Mishra, and Raghunathan 2004; Malhotra and Kubowicz Malhotra 2011; Martin, Borah, and Palmatier 2017), with the negative effect becoming stronger when the security breach becomes more severe, i.e., more victims or more data leaked (Acquisti, Friedman, and Telang 2006; Martin, Borah, and Palmatier 2017). Moreover, owing to spillover effects, firms' stock prices might decrease when competing

firms suffer a security breach, although this spillover effect reverses when the security breach becomes more severe (Martin, Borah, and Palmatier 2017). In addition to affecting stock prices, security breaches also directly affect consumers. They raise consumers' general privacy concern (Bansal, Zahedi, and Gefen 2015; Malhotra, Kim, and Agarwal 2004; Mosteller and Poddar 2017; Smith, Milberg, and Burke 1996, see also below), and preliminary evidence suggests that when confronted with a security breach consumers are more inclined to falsify information, commence in negative WOM, and even switch firms (Martin, Borah, and Palmatier 2017).

Examining consumers' behavioral reaction towards security breaches in more detail, future research should assess how firms can diminish the negative effect of security breaches. With regard to stock prices the adverse effect of a security breach has shown to be less severe when a third party rather than the focal firm is held responsible or when the security breach is caused by an accident rather than a deliberate attack (Acquisti, Friedman, and Telang 2006). Moreover, firms that are transparent about their privacy practices and provide consumers with control over these practices in general (see below), even before outsiders gain unauthorized access, suffer less from the impact of a security breach (Martin, Borah, and Palmatier 2017). Whether these possibilities also affect the impact of a security breach on the way consumers behave remains to be seen.

### *2.4.2 Safe storage*

In line with risk theory (Peter and Tarpey 1975), firms have two options for lowering the risk of security breaches. One is to decrease the impact of security breaches for consumers by reducing the potential loss for consumers, for example by storing less or less sensitive information. The impact of a security breach can also be diminished by anonymizing or aggregating the information (Verhoef, Kooge, and Walk 2016). Anonymization requires that firms remove the link between a person and that person's information, by removing

identifying information such as name or e-mail address (Acquisti, Taylor, and Wagman 2016). Aggregation means that information about consumers is stored at the group or segment level, which per definition implies that the information is anonymous. While anonymization or aggregation ensures that individual consumers are not harmed when information falls into the hands of unknown outsiders, the downside is that it limits a firm's ability to create additional value using the information (Schneider et al. 2017), although there are possibilities to take full advantage of consumer information while simultaneously protecting consumers' privacy (Holtrop et al. 2017).

The alternative is to make security breaches less likely by decreasing the likelihood of a negative event. Firms might store the information for a shorter period, or assure consumers that their information is collected and stored in a '*safe*' environment (Hann et al. 2007). For example, Dutch telecom operator KPN tried to convince consumers that its cloud services were less likely to result in privacy issues because its servers were located in the Netherlands and thus fell under the EUs strict data protection regulation (BTG 2012). While these measures might diminish the likelihood of a security breach, the pledge to store information in a '*safe*' environment only works when consumers are convinced an environment is safer (Sutanto et al. 2013), and thus believe that a privacy breach or violation is indeed less likely in that environment. Future research should not only focus on examining how information storage affects consumers in general, but also make more specific what convinces consumers that information storage is '*safe*'.

**Proposition 5**: Consumers are more willing to let firms store information when firms promise to store (1) less or less sensitive information, (2) only anonymized or aggregated information, (3) information for a shorter period, or (4) information in a safe environment.

## 2.5 Information use

### *2.5.1 Aggregated level vs. Individual level*

Once collected (and stored), firms use the information about consumers for various purposes. As for the collection and storage of information, the use of information only affects consumers when firms clearly inform them as to how the information is used, or when the use of information is evident to consumers. On an aggregated level, firms use consumer information to monitor or optimize internal processes, or to enhance their understanding of the needs and preferences of consumers (Wedel and Kannan 2016). Besides being less evident to consumers, such information use has limited impact on consumers' privacy because it does not rely on personal information, and therefore the influence on consumers is often negligible. Even when firms notify consumers about using information on an aggregated level consumers are inclined to accept as long as they consider it beneficial to themselves. As an example, consumers accept the use of RFID tags in retail outlets when firms use the information to reduce empty shelves (Smith et al. 2014).

On an individual level, besides that firms need information about consumers in order to deliver products or notify consumers about changes in their service, they have begun using the information about consumers for personalization. Personalization implies that firms tailor their offerings of products and services to the needs and preferences of individual consumers (Adomavicius and Tuzhilin 2005; Montgomery and Smith 2009). The growing digitalization enables firms these days to personalize their entire marketing mix: product or service, price, promotion, place or location (Rust and Huang 2014). While consumers might oppose personalization when (they believe) it puts them at a disadvantage – that is, when they have to pay more or receive inferior services compared to other consumers (Lacey, Suh, and Morgan 2007) – our focus will be on how privacy (concern) might affect the approval of personalization (Montgomery and Smith 2009; Rust and Huang 2014).

### *2.5.2 Personalization of product or service*

In order to differentiate themselves from their competitors firms continuously search for ways to use information to augment their service. For example, firms might remember contact details or payment preferences in order to expedite the checkout (Acquisti and Varian 2005). These enhanced services benefit both firms and consumers—consumers from improved service, firms from more loyal and committed customers (Coelho and Henseler 2012). Consumers are more (less) inclined to show promotion-focused (prevention-focused) behavior when firms use the information in order to personalize the website interface (Wirtz and Lwin 2009). Moreover, website morphing, which entails personalizing websites to individual consumers, has a positive effect on consumers' purchases (Hauser et al. 2009; Hauser, Liberali, and Urban 2014). In addition, consumers respond positively to personally recommended music (Chung, Rust, and Wedel 2009) and news (Chung, Wedel, and Rust 2016). Anecdotal evidence suggests that besides personalized recommendations, such as Amazon's "*recommended for you*", LinkedIN's "*suggested connections*", or Netflix' "*selected for you*", consumers also appreciate other forms of personalized content or insights, such as Fitbit's "*fitness insights*" or Siemens's "*smart energy meter*".

However, even when consumers are not always aware which information firms need for these personalized services, the amount and type of information does influence consumers' acceptance of personalization. More specifically, consumers value personalized service less when it is based on sensitive information (Mothersbaugh et al. 2012), and preliminary evidence shows that for recommendation systems consumers only disclose information when they expect valuable recommendations (Knijnenburg and Kobsa 2013). Moreover, while external information – such as derived from social media – could improve personalization (Chung, Wedel, and Rust 2016), even in the context of scientific research many respondents were hesitant to provide access to such information to improve product

recommendations (Heimbach, Gottschlich, and Hinz 2015). The context of search-and-discovery services, such as FourSquare or Gowalla, provides further evidence that consumers' acceptance of personalized services depends on which information is needed (Xie, Knijnenburg, and Jin 2014). While, in line with the privacy calculus, consumers seem to balance the positive and negative consequences of personalized services, future research should assess when and for which consumers the benefits outweigh the '*costs*'.

### *2.5.3 Personalization of price*

Besides personalized products or services, firms have begun providing consumers personalized discounts or rewards, and even personalized prices (Acquisti and Varian 2005). While consumers have shown to value personalized discounts less when based on sensitive information—discounts for '*embarrassing*' products (White 2004)—consumers primarily reject personalized pricing because they consider such price differences unfair (Feinberg, Krishna, and Zhang 2002). Rather than being worried about their privacy consumers disapprove personalized pricing because they fail to understand why they pay more than other consumers. Therefore, even though personalized promotions might benefit firms (Khan, Lewis, and Singh 2009; Zhang and Wedel 2009), anecdotal evidence about firms experimenting with personalized pricing (e.g., outrage over Amazon's variable pricing dropped their stock price by more than 13%, CNN 2005) shows that firms might suffer from future backlash when consumers eventually find out they are paying more.

### *2.5.4 Personalization of promotion*

Although the personalization of online (banner) advertisements and direct mailings to individual consumers has become standard practice, consumers have shown mixed feelings towards the personalization of marketing communication. While a majority of US consumers rejects behavioral targeting (Purcell, Brenner, and Rainie 2012), consumers also consider personalized marketing content more relevant and useful, thereby making banner ads and

direct mails more effective (Aguirre et al. 2015; Ansari and Mela 2003; Bleier and Eisenbeiss 2015a; b; Van Doorn and Hoekstra 2013; Goldfarb and Tucker 2011b; Tucker 2014).

However, too much personalization makes marketing communication intrusive and triggers privacy concerns (Van Doorn and Hoekstra 2013; Edwards, Li, and Lee 2002; Li, Edwards, and Lee 2002). As consumers become cognizant information is collected and used, reactance theory suggests consumers are bothered by a lack of control over the collection or use of information for personalized marketing communication. Besides that ads become more intrusive when they are cognitively intense or incongruent with the website (Edwards, Li, and Lee 2002; Li, Edwards, and Lee 2002), intrusiveness is induced when firms openly use detailed information about individual consumers in their ads (Aguirre et al. 2015; Van Doorn and Hoekstra 2013). Targeting ads to an individual consumer (Tucker 2014) or showing the exact same product the consumer saw before, so-called dynamic retargeting, also makes online ads less effective (Bleier and Eisenbeiss 2015b; Lambrecht and Tucker 2013), as consumers become aware that personal information is being collected, stored, and used (Bleier and Eisenbeiss 2015b).

As also discussed below, firms can conserve the effectiveness of personalized marketing communication by becoming more transparent with regard to the (creation of) personalized marketing communication (Aguirre et al. 2015) or by providing consumers more control over information disclosure (Tucker 2014). Moreover, firms could alter their marketing communication to try and reduce the arousal of privacy concerns. While not showing the exact same product twice (Bleier and Eisenbeiss 2015b; Lambrecht and Tucker 2013) and increasing the target audience of banner ads could prevent arousing privacy concern (Tucker 2014), it would also diminish the match with individual consumers (and thus the effectiveness). In line with regulatory focus theory (Higgins 1997), a better solution would be to try and let consumers focus on the benefits by increasing the relevance of marketing

communication. For example, personalizing online banner ads becomes more effective when a banner ad is more relevant to the consumer (Lambrecht and Tucker 2013), and mobile ads become less intrusive (and more effective) when these ads are relevant with regard to the physical location of the consumer (Luo et al. 2014).

**Proposition 6**: Firms can prevent arousing privacy concern or intrusiveness and preserve the increase in effectiveness of personalized marketing communication by making marketing communication, such as banner ads and direct mail, more relevant.

### *2.5.5 Personalization of place or location*

A recent development is that the rise of mobile devices enables firms to personalize the location where they offer their products or services. Location-based services tailor content to consumers' physical location, thereby providing consumers with the convenience of receiving content at the right time and location (Xu et al. 2009, 2011; Zhao, Lu, and Gupta 2012). This content can range from location-specific information, such as weather reports, to location-specific advertisements or coupons. Given that location tracking has only recently risen in prominence few studies have assessed the acceptance of such location-based service.

However, as also discussed above consumers are vigilant about firms tracking offline behavior, and a majority of consumers still rejects location-based advertising (Urban and Hoofnagle 2014). Therefore, firms need a better understanding on when consumers value the savings in time or effort enough to offset their worries about firms tracking their location. What seems to matter most to consumers is whether the content firms provide is truly relevant to them, as the intention to disclose information to location-based services is explained more by the benefits (incentives, possibility to interact) than the costs (privacy concern) (Zhao, Lu, and Gupta 2012). Even more than online personalization location-based services might give consumers the feeling they are being followed and watched. Firms can prevent triggering such feelings by making the information truly relevant, in terms of time and geographic location

(Luo et al. 2014). Thus, as long as firms provide relevant content consumers are influenced less by negative feelings with regard to location tracking.

### *2.5.6 Third-party sharing*

Besides using information internally, firms also generate revenue by selling information or customer intelligence to other firms. Consumers oppose sharing and selling information to unknown third parties (Alreck and Settle 2007), as they believe they are more at risk (Jai, Burns, and King 2013), most likely because they do not know (transparency) or cannot influence (control) how their information will be used. Moreover, third-party firms typically have no incentive to provide consumers with any suitable benefit in return. As a result, consumers respond negatively to firms selling information, for example by complaining, refusing information disclosure, or avoiding marketing communication, whereas their long-term commitment and loyalty are enhanced when firms refuse to sell information to third parties (Wirtz and Lwin 2009). Although firms could try and appease consumers' concerns, for example by disseminating information with less detail, the issue is that this decreases the potential benefit of information sharing (Schneider et al. 2017).

## 2.6 Transparency

### *2.6.1 Effect on consumers*

Over the past decades, pressure from legislators and consumer protection commissions have mandated firms to be more transparent about their privacy practices. In line with social contract theory, transparency enhances the relationship between firms and consumers as it ensures a '*fair exchange*' of information (Culnan and Bies 2003). Therefore, transparency decreases the extent to which consumers feel their privacy is violated (Martin, Borah, and Palmatier 2017), and makes consumers more willing to disclose information (Son and Kim 2008) or even purchase products (Schlosser, White, and Lloyd 2006).

Social contract theory also suggests that firms could benefit long-term when consumers consider them transparent due to enhanced trust and commitment (Culnan and Bies 2003). Transparency could prevent future discontent with firms' privacy practices, as consumers know or could have known how their privacy was handled. This shifts (part of) the responsibility for future privacy issues or the '*locus of control*' from the firm to the consumer. Likewise, when firms explain their privacy practices, consumers are less likely to regret giving permission to collect, store, or use their information, as it increases the correspondence between consumers' intentions and their behavior (Zimmer et al. 2010). Future research should examine this (long-term) effect more carefully, and assess whether and why consumers become more committed and loyal to firms they consider transparent.

**Proposition 7**: Transparency about how consumers' privacy is handled diminishes future discontent with firms' privacy practices.

### *2.6.2 Privacy statement and seal*

To notify consumers about the collection, storage, and use of information most firms post a privacy statement, which is a written overview of their privacy practices generally available on their website. An issue for firms is that consumers do not always take the effort to understand how firms handle their privacy. Especially online or on mobile devices consumers have to make many decisions within a short period of time, and are faced with too much information about their privacy ('*information overload*'), which makes it difficult to understand which information is collected and stored, and how firms use this information (Metzger 2007). Moreover, some consumers consider privacy not important enough to invest time in understanding a firm's privacy practices (Dinev, McConnell, and Smith 2015). Therefore, rather than reading privacy statements (Eurobarometer 2011) consumers use them as a heuristic instead. In line with signaling theory (Boulding and Kirmani 1993) prior studies have shown that the mere presence of a privacy statement increases consumers' trust in a firm

(Aljukhadar, Senecal, and Ouellette 2010), willingness to disclose information (Hui, Teo, and Lee 2007; Wang, Beatty, and Foxx 2004; Xie, Teo, and Wan 2006), and even willingness to purchase (Aljukhadar, Senecal, and Ouellette 2010). However, given that privacy statements are mandated in most countries, the actual differentiating effect on how consumers behave is probably limited.

Likewise, firms post privacy seals, such as TRUSTe or BBBOnline, to try and convince consumers that their privacy is secure. Although some studies show that privacy seals give consumers the feeling that firms are transparent (Kim and Kim 2011; Rifon, LaRose, and Choi 2005) and increase trust more than other objective trustmarks (Aiken and Boush 2006), other studies show that the effect on consumers' willingness to disclose information is small (Wang, Beatty, and Foxx 2004) or absent, despite consumers' familiarity with the seal (Hui, Teo, and Lee 2007). Still, another study confirms that when choosing between firms consumers opt for the firm with a privacy signal, such as a privacy icon or a link to their privacy statement, even when that firm is more expensive (Tsai et al. 2011).

### *2.6.3 Arousal of privacy concern*

Another (related) reason firms struggle with transparency is that privacy is not always top-of-mind, especially online or when consumers use mobile devices. Mentioning privacy, information collection, or other 'sensitive' terms (e.g., behavioral targeting, RFID) triggers consumers' privacy concerns. For example, respondents disclose less information in surveys when privacy is mentioned (Acquisti, John, and Loewenstein 2012), and consumers are less willing to adopt a tracking system in a grocery store when RFID is in the name (Smith et al. 2014). In fact, consumers consider the negative outcomes ("*information will be used against me*") more likely when firms explain both benefits and risks of information disclosure (LaRose and Rifon 2007), worry more about their privacy when '*data mining'* is explained (Bolderdijk, Steg, and Postmes 2013), and pointing out a privacy policy on an online social

network decreased consumers' willingness to disclose their location (Knijnenburg, Kobsa, and Jin 2013).

Nevertheless, as firms are mandated to explain their privacy practices, a better understanding how to handle the adverse effect of transparency is essential. One solution could be that when firms trigger consumers' privacy concern they need to convince consumers that they rigorously protect privacy or that consumers have control over their information (see below). One possibility would be to make privacy statements look '*strong*', for example by promising confidentiality and guaranteeing protection against information theft (Schlosser, White, and Lloyd 2006). Similarly, posting a privacy seal in addition to explaining the benefits and risks of information collection reduces the perceived risks (LaRose and Rifon 2007), as that also provides consumers some assurance.

**Proposition 8**: Firms can resolve (part of) the issue of privacy arousal by using signals that give consumers the feeling they are protected.

#### *2.6.4 Explaining the benefits*

Regulatory focus theory suggests that another solution for the issue of privacy arousal could be to stress the benefits of information collection and use in order to direct consumers' attention towards these benefits (Higgins 1997). For example, when the benefits of RFID are stressed consumers consider RFID more useful, while stressing the negative side makes consumers more worried about their privacy (Smith et al. 2014). Recently, several news outlets (e.g., *Bild, The Guardian, Forbes*) have begun using pop-up announcements to explain how the collection of information enables them to both supply news for free and provide consumers with news that fits their needs. Consumers feel less vulnerable when firms justify the use of personal information (Aguirre et al. 2015), and this feeling of security increases the click-through intention for personalized banner ads (Aguirre et al. 2015) as well as for personalized mail (White et al. 2008). Likewise, explaining the benefits of behavioral

targeting to consumers increases the acceptance and actual click-through of targeted banner ads (Schumann, Von Wangenheim, and Groene 2014).

However, if firms want transparency to be helpful they have to understand when consumers take the effort to understand their explanations of the benefits, and how to motivate consumers in case they take little or no effort to understand these explanations. One easy solution is to make privacy statements with the costs and benefits short and easy to read (Pan and Zinkhan 2006), rather than using juridical language even lawyers cannot understand. Another possibility to make things easier for consumers would be to explain privacy practices and the way consumers benefit in short, easy-to-follow videos, as implemented by news outlet *The Guardian*. Preliminary evidence suggests that posting a video could enhance consumers' trust in the firm and (indirectly) their intention to transact with that firm (Aljukhadar, Senecal, and Ouellette 2010). Furthermore, White and colleagues (2014) suggest that firms could benefit from first explaining the negative consequences to consumers (e.g., "*information collection decreases your anonymity*") before explaining the positive consequences (e.g., "*you get a discount*"), as that enhances consumers' willingness to disclose information.

Besides motivating consumers to invest time in understanding firms' privacy practices firms also need to decide what they communicate. Besides the aforementioned influence of the collection and storage of information, firms need to understand which benefit(s) derived from the use of information consumers appreciate the most. For example, when justifying the collection of personal information for behavioral targeting, rather than stressing the increased relevance of banner ads, firms are better off emphasizing that collection allows free products or services (Schumann, Von Wangenheim, and Groene 2014). Besides stressing the right benefits, Martin and colleagues (2017) suggest that transparency only benefits firms when they also provide consumers control.

**Proposition 9**: Firms can resolve (part of) the issue of privacy arousal by stressing the (right) benefits to consumers.

## 2.7 Control

### *2.7.1 Effect on consumers*

As for transparency, pressure from legislators and consumer protection commissions have mandated that firms provide consumers control over their information. Being focused on informed consent and providing consumers the "*right to erasure*", the EU government in particular intends to give consumers more control over '*their*' own information (General Data Protection Regulation (EU) 2018). Social contract theory suggests that firms benefit from providing control, considering it is another important requirement for a '*fair exchange*' of information between firms and consumers (Culnan and Bies 2003). When consumers believe a firm provides control over (secondary) use they trust the firm more (Mosteller and Poddar 2017) and feel less vulnerable (Martin, Borah, and Palmatier 2017). Therefore, consumers are more inclined to choose that firm (Hann et al. 2007; Phelps, Nowak, and Ferrell 2000), more cooperative and committed towards that firm (Mosteller and Poddar 2017; Son and Kim 2008), and more willing to disclose (sensitive) information for a personalized service (Mothersbaugh et al. 2012). Moreover, control over the storage of information enhances the acceptance of behavioral advertising (Schumann, Von Wangenheim, and Groene 2014), and on Facebook the effectiveness of banner ads even increased after they made it easier for it's users to control their privacy (Tucker 2014).

Although it has been shown convincingly that consumers are positively influenced by (perceived) control, future studies should assess why consumers become more cooperative and committed. Prior research has suggested that control provides consumers with a sense of autonomy, which matters since consumers react negatively when they are confined in their choices (Brehm 1966). Related to this is that control might make consumers feel less

vulnerable (Martin, Borah, and Palmatier 2017) as it allows consumers to revoke these choices whenever they please, making their choices less consequential.

**Proposition 10**: Control over information makes consumers more cooperative and committed, because (1) control provides them with a sense of autonomy, and (2) it makes decisions less consequential.

### *2.7.2 Disruption of information collection*

Up until now, despite the mounting legislative pressure, firms have remained reluctant to provide control. The main reason for this reluctance seems that if they allow consumers to disrupt the collection, storage, or use of personal information it could prevent firms from taking full advantage of customer intelligence and '*big data*'. However, there has been hardly any research on the extent to which consumers actually use their ability to control the collection, storage, and use of information.

Preliminary evidence shows that consumers already become more cooperative by a feeling of control over the use of information (Brandimarte, Acquisti, and Loewenstein 2013). This seems to suggest that consumers are not so much interested in disruption, but rather in having the ability to disrupt in case this is needed. Future research should assess to what extent consumers would make use of their ability to control the collection, storage, and use of information. For now, we can only conclude that consumers are expected to disrupt the collection, storage, and use of personal information when the harmfulness of a firm's privacy practices (e.g., selling sensitive information to third parties) exceeds the benefits they offer.

### *2.7.3 Control over stored information*

Besides increasing commitment and loyalty to a firm providing control could create another mutual benefit. Consumers are worried that firms' databases contain errors (Smith, Milberg, and Burke 1996), either because enriching consumer profiles using inferences results in

accidental mistakes or due to consumers providing erroneous information themselves. Firms can avoid such issues by making information provision voluntary (Norberg and Horne 2014), and can also solve such issues by giving consumers access to their personal information and allowing them to correct any potential errors (Hann et al. 2007). As an example, Google increasingly allows users to alter (improve) the profiles used for personalized advertisements with regard to consumers' interests and preferences.

### *2.7.4 Information disclosure as default*

Another important issue for firms remains '*how'* they should provide consumers with control. Offering an opt-out choice results in more consumers consenting to provide information than an opt-in choice (Johnson, Bellman, and Lohse 2002), while it has no effect on consumers' purchase likelihood (Eastlick, Lotz, and Warrington 2006). However, legislators tend to force a choice of opting in rather than opting out. Besides legislative pressure firms also have to be aware that an opt-out choice, which essentially makes information disclosure the default, will result in more cases in which they collect, store, and use information against the will of the consumer. Therefore, while firms might benefit in the short term—consumers initially consent—it could negatively affect consumers' satisfaction and long-term commitment.

To the contrary, control could prevent future discontent with firms' privacy practices as it shifts (part of) the responsibility for future privacy issues or the '*locus of control*' from the firm to the consumer. If firms provide control over information, and consumers make no use of this control, consumers can only blame themselves when firms' privacy practices are not in line with their preferences. In line with this reasoning, preliminary evidence suggests that control in conjunction with transparency is most effective in decreasing feelings of emotional violation and increasing trust, as well as in decreasing the negative effect of a privacy breach (Martin, Borah, and Palmatier 2017). Future research should examine in more detail how firms could best provide control in a way that does not antagonize consumers.

**Proposition 12**: Firms that have information collection as the default (e.g., use an opt-out choice for information collection) will suffer from (more) dissatisfied customers.

## 2.8 Firm characteristics

### *2.8.1 Industry*

Consumers' privacy preferences and expectations differ between contexts (Martin and Nissenbaum 2016a; Nissenbaum 2004). Therefore, the influence of privacy practices on consumers differs between industries (or sectors). Privacy is a more pressing issue in industries that rely on collecting a large amount of information or sensitive information, such as healthcare providers or banking. Hence, all features that decrease privacy concerns or increase trust are more important in fostering consumers' willingness to disclose information, and, more generally, their willingness to interact or transact with firms from those industries (Bart et al. 2005; Pan and Zinkhan 2006).

Besides the sensitivity of information, consumers take into account whether the information that is collected, stored, and used is congruent with the products or services of a firm. Consumers are more willing to disclose particulars when they anticipate they will be asked to disclose that information (White, Novak, and Hoffman 2014). Thus, collecting sensitive specifics is less of an issue when the information is congruent with the firm's products or services. For example, while consumers accept that financial institutions will collect details about their income or mortgage they are reluctant to disclose their medical condition (Lwin, Wirtz, and Williams 2007; Martin and Nissenbaum 2016a).

Moreover, the industry (or sector) also moderates the influence of security breaches, although these findings have not always been consistent. Acquisti and colleagues (2006) show that the effect on firms is more severe for retail firms than for other firms (e.g., financial), while Malhotra and Malhotra (2011) provide evidence that the effect is stronger for financial firms than for other firms (e.g., retail). Moreover, Cavusoglu and colleagues (2004) showed

earlier that the effect is more severe for online firms than for offline firms, most likely because for online firms there is more information to be lost. While these findings are all focused on stock prices future research should assess whether the direct influence of security breaches on consumers also differs between industries.

### *2.8.2 Reputation*

Besides the industry several other firm characteristics influence consumers. All characteristics of firms or websites that signal competence and quality, in particular their reputation, motivate consumers to disclose information (Aiken and Boush 2006; Bart et al. 2005; Lwin, Wirtz, and Stanaland 2016; Schoenbachler and Gordon 2002; Xie, Teo, and Wan 2006).

Reputation also moderates the influence of firms' privacy practices. On the one hand, privacy statements are more effective for firms with a strong reputation (Xie, Teo, and Wan 2006), as consumers have more confidence in the credibility of these statements. On the other hand, transparency is considered more crucial for firms with a weak reputation (Joinson et al. 2010). More specifically, a lack of justification regarding the origin of the information in personalized banner ads only makes consumers feel vulnerable on untrustworthy websites, such as Facebook (Aguirre et al. 2015). Likewise, as a strong reputation already convinces consumers to accept information collection, providing a monetary compensation becomes ineffective in convincing consumers to disclose information (Xie, Teo, and Wan 2006).

Besides signaling benevolence and integrity, the reputation of a firm might also allude to competence and ability to provide consumers with valuable products and services (McKnight, Choudhury, and Kacmar 2002). Having a reputation of competence may therefore enhance the influence of the potential benefits of collection, storage, and use of information. For example, consumers were more convinced that personalization is valuable when it is provided by firms with a strong reputation (Bleier and Eisenbeiss 2015b). Future research

should focus on providing a better understanding how the influence of privacy practices on consumers is moderated by firm characteristics.

## 2.9 Consumer characteristics

### *2.9.1 General privacy concern*

Consumers differ in the extent to which they value their privacy (Larson and Bell 1988; Laufer and Wolfe 1977), implying that some consumers worry more about their privacy in general than others. This differs between generations, with older consumers being more concerned about their privacy (Bellman et al. 2004; Goldfarb and Tucker 2012). Moreover, females (Bellman et al. 2004; Goldfarb and Tucker 2012) and consumers with a low education (Milne and Boza 1999) are generally more apprehensive about their privacy, as are consumers who have experienced a privacy violation (Bansal, Zahedi, and Gefen 2015; Mosteller and Poddar 2017). Meanwhile, having experience with more channels or devices has both been linked to higher (Sheehan and Hoy 2000) and lower privacy concern (Bellman et al. 2004). While experienced consumers are more aware of the risks (higher privacy concern), they also understand how to protect against these risks (lower privacy concern). Future work should explore the role of (digital) experience in more detail.

Evidently, consumers who worry more about their privacy in general are less willing to disclose information (Premazzi et al. 2010; Zhao, Lu, and Gupta 2012) and more inclined to protect their privacy (Korzaan and Boswell 2008; Milne and Culnan 2004). Moreover, they are less receptive to products and services that rely on collecting personal information, such as loyalty programs, CRM, and behavioral targeting (Ashley et al. 2011; Awad and Krishnan 2006; Schumann, Von Wangenheim, and Groene 2014; Taylor, Ferguson, and Ellen 2015). Based on general privacy concern consumers have also been divided into three segments: privacy fundamentalists, privacy pragmatists, and those unconcerned about privacy (Ackerman, Cranor, and Reagle 1999; Dolnicar and Jordaan 2007; Hogan, Lemon, and Rust

2002; Kumaraguru and Cranor 2005; Westin 1967). However, segmenting consumers based on (general) privacy concern is much disputed (Hoofnagle and Urban 2014; Martin and Nissenbaum 2016b), as several context- and situation-specific elements prevent these segments from accurately differentiating how consumers behave (Acquisti and Grossklags 2005a; King 2014; Urban and Hoofnagle 2014). While an extensive discussion on privacy segmentation is out of the scope of this dissertation, future research should examine segmenting based on (general) privacy preferences more thoroughly.

As general privacy concern reflects the importance of privacy (involvement) for consumers (Bansal, Zahedi, and Gefen 2008, 2015), it could also moderate the influence of firms' privacy practices. The (positive) influence of personalized service is weaker for consumers who are highly concerned about their privacy (Shen and Dwayne Ball 2009), while the (negative) influence of information sensitivity is stronger for these consumers (Mothersbaugh et al. 2012). Moreover, while highly involved consumers are more affected by transparency and other privacy-protective features (Awad and Krishnan 2006; Bansal, Zahedi, and Gefen 2008), they are not convinced by '*weak*' privacy signals such as privacy seals (Kim and Kim 2011). Future research should assess in more detail whether general privacy concern enhances or diminishes the effect of privacy protective features.

### *2.9.2 Innovativeness, propensity to trust, and personal circumstances*

Besides privacy concern several other consumer-specific characteristics affect how consumers deal with firms' privacy practices. For example, innovative consumers are more inclined to accept innovations than others, also when these innovations are contingent on the collection and use of information (Xu et al. 2009, 2011; Zhao, Lu, and Gupta 2012). In fact, innovative consumers are more receptive to firms collecting and using their information in general (Mothersbaugh et al. 2012; Xu et al. 2011).

The same holds for consumers with a high propensity to trust others (Dinev and Hart 2006; Hui, Teo, and Lee 2007; Malhotra, Kim, and Agarwal 2004; Mothersbaugh et al. 2012), as they are more convinced than consumers with a low propensity to trust others that firms will not misuse or exploit their information (Aljukhadar, Senecal, and Ouellette 2010; Kim, Ferrin, and Rao 2009).

Furthermore, consumers' personal circumstances affect the influence of firms' privacy practices. Whether a consumer considers information to be sensitive may be based on his or her personal situation, with the importance of keeping information away from firms dependent on the extent to which a consumer believes he or she has something to hide. For example, while most consumers are unwilling to disclose medical information, a consumer in poor health may feel particularly strongly about this issue (Bansal, Mariam, and Gefen 2010). A better understanding how a consumer's personal circumstances affect the influence of a firm's privacy practices would be highly valuable for firms.

### *2.9.3 Experience*

Besides consumers' personality and personal circumstances, also their relationship with firms matters. Whether consumers trust a firm, and thus accept information collection and use, revolves around their prior experience with that firm (Bansal, Zahedi, and Gefen 2015; Bart et al. 2005; Chellappa and Sin 2005; Schoenbachler and Gordon 2002).

However, even though consumers are generally more willing to disclose information to a firm they have a (long) relationship with, they are less willing to disclose embarrassing information to these firms for fear of losing face (White 2004). Moreover, offering monetary compensation makes consumers with positive experiences with a firm less inclined to disclose information (Premazzi et al. 2010). One reason for this negative effect, which demands further investigation, could be that providing monetary compensation makes information disclosure more of a financial decision than a decision based on mutual trust. Therefore,

offering monetary compensation when consumers have had positive prior experiences might give them the feeling that information disclosure is not in their best interest.

## 2.10 Environment characteristics

### *2.10.1 Cultural differences*

Privacy and privacy concern relate to cultural differences, as consumers in individualistic countries worry more about their privacy (Milberg, Smith, and Burke 2000), making perceived privacy and security (more) important drivers for the perceived value of a website (Steenkamp and Geyskens 2006). However, as in a more recent study individualism has also been linked to a lower privacy concern (Lowry, Cao, and Everard 2011), more insights on the influence of culture on privacy (concern) is required.

Importantly, consumers from different countries and cultures worry about different issues (Gurau and Ranchhod 2009; Miltgen and Peyrat-Guillard 2014). For example, for US consumers unauthorized secondary use is a minor issue, whereas for Singaporean consumers this is the most important privacy violation when dealing with online retailers (Hann et al. 2007). Since most knowledge is based on US-based samples, future work should assess these differences in more detail.

### *2.10.2 Legislation*

National differences are also reflected in legislation (Bellman et al. 2004; Milberg, Smith, and Burke 2000), and in countries for which the rule of law is very formal, and strict, privacy and security features are less important drivers for the perceived value of a website (Steenkamp and Geyskens 2006). Moreover, while US legislation is focused on letting firms and consumers negotiate fairly over the collection, storage, and use of personal information (Ohlhausen 2014), the European Union has become more protective over the past decade, as evidenced by the upcoming General Data Protection Regulation. As these differences affect

firms' potential to collect, store, and use information (Goldfarb and Tucker 2011a), focusing on consumers' individual wishes is not enough, as firms' privacy practices should also be in line with national laws (Nissenbaum 2004). While discussing privacy legislation and its influence on firms is out of scope, future research should carefully assess how both current and future privacy legislation affect firms' privacy practices.

Consumers are not always aware how legislation protects their privacy. Nevertheless, since consumers worry less when they believe they are protected by the law, they become more willing to provide information, less inclined to fabricate information, and less inclined to actively protect their privacy (Lwin, Wirtz, and Williams 2007). Moreover, while it has been suggested that the presence of legislation becomes less important when firms provide control (Xu et al. 2009), another study suggests the effect is the other way around—providing control becomes less effective in the presence of legislation (Xu et al. 2012). Future research should examine this interplay between privacy legislation and control, and its influence on consumers, in more detail.

### *2.10.3 Privacy-enhancing technologies*

Consumers have recently begun taking matters in their own hands by using privacy-enhancing technologies (PETs) that offer options for privacy, such as browser extensions and cookie blockers. Even when not all consumers have access to these technologies, we expect they will affect the influence privacy practices have on consumers. As an example, giving consumers control would be less effective when consumers are able to use PETs that provide them control over the collection, storage, or use of information. While prior studies have assessed what determines whether PETs are used (e.g., perceived ease-of-use, perceived usefulness) (Xu, Crossler, and Bélanger 2012), understanding how these PETs affect firms and the relationships with their customers remains an important area for future research.

## 2.11 Summary and directions for future research

As firms increasingly collect, store, and use information about consumers, privacy concerns have surged. Given the importance of consumer information to firms, understanding how privacy affects consumers is crucial. Drawing on insights from various fields, we review relevant findings with regard to the effect of firms' privacy practices on consumers. Table 2-2 provides an overview of these findings, while Table 2-3 describes how some of these effects are moderated by differences between firms, consumers, and environments.

On the basis of this review, we have formulated several propositions with regard to the influence of firms' privacy practices that should provide direction for future research. On a more general level, more research should be devoted to how consumers trade off the negative and positive consequences of information disclosure (the privacy calculus) in specific contexts, and in which circumstances consumers behave in accordance with this tradeoff. Future research should (1) identify the negative and positive consequences of information collection, storage, and use, (2) assess the extent to which consumers are aware of these consequences, (3) reveal the impact of these consequences, and (4) use field studies to link these consequences to relevant behavioral outcomes, ranging from accepting information collection to churn and word of mouth. Except for some recent studies on online advertising, most findings are based on scenarios and intentions ("*what would you do?*") rather than actual behavior. Linking consumers' privacy calculus or their intentions to actual behavior should also result in a better understanding of when and why the privacy paradox occurs or whether it is due to inherently inconsistent consumer behavior.

**Table 2-2**. Current knowledge about consumer privacy (main effects)

| Topic | Findings | Main papers |
|---|---|---|
| Information collection | - Consumers are less inclined to disclose information when firms request more (sensitive) information<br>- Consumers are more inclined to accept information collection by computers than humans (e.g., employers)<br>- Consumers are more inclined to disclose information when they receive monetary compensation, although this response depends on the type of information and the amount of compensation<br>- Consumers are more inclined to disclose information when firms disclose information first, when privacy (concern) is not triggered, or when other consumers disclose similar information | Acquisti et al. (2012; 2013); Hui et al. (2007); Martin et al. (2017); Milne et al. (2017); Mothersbaugh et al. (2012); Premazzi et al. (2010); Schwaig et al. (2013); White (2004) |
| Information storage | - Consumers worry that unknown outsiders may get access to their personal information<br>- Privacy breaches, both the firm's own and that of a competitor, can negatively affect stock prices | Acquisti et al. (2006); Martin et al. (2017); Sutanto et al. (2013) |
| Information use | - Consumers are affected less when information is used at an aggregated level<br>- Consumers value personalization less when it demands they have to provide additional information or when it is based on sensitive information<br>- Consumers click (and buy) more when banner ads and direct mail are personalized, unless these ads or mails arouse privacy concerns by making it obvious that firms collect, store, and use consumers' information<br>- Consumers are less committed and loyal to firms that share or sell information with (unknown) third parties | Bleier and Eisenbeiss (2015a; 2015b); Goldfarb and Tucker (2011b); Coelho and Henseler (2012); Lambrecht and Tucker (2013); Tucker (2014); Wirtz and Lwin (2009); Xie et al. (2006); Xu et al. (2009; 2011); Zhao et al. (2012) |

| | | |
|---|---|---|
| Transparency | - Consumers are more committed and cooperative towards transparent firms<br>- Consumers do not always take the time to understand how firms handle their privacy, and use privacy statements (and seals) as heuristics instead<br>- Consumers do not always think about privacy, which is why privacy statements (or other sensitive terms) can arouse consumers' privacy concerns<br>- Consumers are more inclined to accept information collection, storage, and use when firms explain the (right) benefits to them | Aguirre et al. (2015); Aiken and Boush (2006); Aljukhadar et al. (2010); Hui et al. (2007); Martin et al. (2017); Schumann et al. (2014); Son and Kim (2008); Tsai et al. (2011); Wirtz and Lwin (2009); Xie et al. (2006) |
| Control | - Consumers are more inclined to choose a firm, disclose sensitive information, or accept personalized ads when (they believe) firms provide control over the collection, storage, and use of information<br>- Consumers accept information collection more often when firms make information collection the default (e.g., opt-out choice) | Acquisti et al. (2013); Hann et al. (2007); Johnson et al. (2002); Martin et al. (2017); Mothersbaugh et al. (2012); Schumann et al. (2014); Tucker (2014) |

Besides being challenged by the collection, storage, and use of personal information, increasing regulatory and technological pressure forces firms to better understand the role of transparency and control. Although one could debate whether informed consent works in practice (Landau 2015; Nissenbaum 2015), it appears to remain the main focus of legislators in both the US and the EU. Therefore, future research should provide insights into (1) the extent to which transparency and control affect actual consumer behavior, (2) in which situations and for which firms and consumers transparency and control are crucial, (3) in which form firms should provide transparency and control, and (4) the long-term

consequences of providing more or less transparency and control. Game-theoretic models suggest that proactive privacy protection is a viable business model (Lee, Ahn, and Bang 2011). However, given the drawbacks of transparency and control it remains to be seen whether this also works in practice.

**Table 2-3.** Current knowledge about consumer privacy (moderators)

| Moderator | Findings | Main papers |
|---|---|---|
| Firm | - The effect of privacy-protective and -invasive features on consumers is more pronounced in industries that rely on collecting sensitive information<br>- The effect of information sensitivity is less pronounced when the information is congruent with the firm's products and services<br>- The effect of monetary compensation on consumers is weaker (or absent) for firms with a strong reputation | Aguirre et al. (2015); Bart et al. (2005); Lwin et al. (2007); Pan and Zinkhan (2006); Xie et al. (2006) |
| Consumer | - The effect of information sensitivity and privacy-protective features (e.g., transparency) is more pronounced for consumers with a high general privacy concern<br>- The effect of the benefits of data-driven innovations is stronger for consumers high on innovativeness<br>- The effect of monetary compensation on consumers' willingness to disclose information is weaker (or absent) when consumers already have a relationship with a firm | Bansal et al. (2010; 2015); Premazzi et al. (2010); Mothersbaugh et al. (2012); White (2004); Xu et al. (2009; 2011); Zhao et al. (2012) |
| Environment | - The effect of privacy-protective and -invasive features on consumers depends on cultural differences<br>- The effect of control on consumers is less pronounced in countries with strong privacy legislation or in the presence of privacy-enhancing technologies (PETs) | Hann et al. (2007); Lwin et al. (2007); Steenkamp and Geyskens (2006); Xu et al. (2009; 2011); Zhao et al. (2012) |

Finally, future research should focus on the differences between consumers and environments. Most studies so far have used student samples from the US to show how firms' privacy practices affect consumers. However, given the differences between generations – for example, older consumers are more concerned – these findings might not be generalizable. Likewise, given that cultural differences exist with regard to privacy—for example, loss of face is more important in Asian culture—cross-cultural studies need to assess how these differences moderate the effect of firms' privacy practices on consumers.

## 2.12 Managerial implications

On the basis of current knowledge summarized in Table 2-2 and Table 2-3, we identify five important managerial implications for firms. First, firms must exercise caution about *'what'* and *'how'* they collect information. Consumers are not only hesitant to disclose sensitive information, such as financial or medical information, but are less responsive to monetary compensation or any other means to convince them to accept information collection. Moreover, while collecting information automatically is more convenient for consumers, these same consumers might also consider it as unfair.

Second, firms should make sure that their information storage is secure. Security breaches reduce firm value (i.e., stock prices), and by damaging a firm's reputation it might also hurt firms in the long run. In addition to preventing security breaches, firms could attempt to decrease the negative impact of any security breach, for example by being transparent in their communication and providing control via adequate channels. Also anonymization of stored information could decrease the risks for consumers, although this only helps when consumers understand that anonymization puts them less at risk.

Third, firms should be aware that the acceptance of profiling and personalization depends on which and how much information is used. Employing personal information in personalized banner ads or direct mailings could trigger privacy concern (and reactance),

which could reduce the effectiveness of these ads or mailings. Yet, firms should also be aware of how the use of information, in particular for personalization, could provide consumers with the convenience of receiving (relevant) content at the right time and location. Overall, a more thorough understanding of the benefits and costs of information use for personalization and other purposes is essential for firms.

Fourth, although firms should ensure that they handle privacy honestly, firms have to take into account that transparency, i.e., communicating about privacy, triggers privacy concerns. Therefore, firms should only mention privacy when consumers have an actual privacy decision to make (e.g., whether to allow information collection), as transparency works best in concurrence with control. Moreover, rather than only convincing consumers they are not at risk, firms should be transparent about how the collection, storage, and use of information benefits consumers.

Finally, for all of these implications holds that firms have to take into account that the influence of privacy practices differs between firms, consumers, and environments. In particular, firms have to be aware that privacy is a more pressing issue in industries that handle either a lot of information or sensitive information. Moreover, firms should realize that some consumers value their privacy more than others, which affects whether they accept information collection, and therefore also the adoption of data-driven products and services. In understanding consumer behavior, it is important to take into account that consumers' privacy preferences are both situation- and context-specific.

## 2.13 Conclusion

Privacy affects firms on the strategic and operational levels regarding product management (e.g., personalization), distribution (e.g., location-based services), pricing (e.g., monetary benefits for providing information), and communication (e.g., transparency). The growing collection of information has triggered consumers' privacy concerns, which has catapulted

privacy from being a minor issue to being an area in great need of more insights. By summarizing current knowledge and formulating research propositions about firms' privacy practices, we provide direction to future research. Although the concept of privacy has changed and will change over time, it will remain an important issue for many years to come.

# Chapter 3

# Consumers' Privacy Calculus: The PRICAL Index Development and Validation

**Abstract**

Collecting personal information about consumers is crucial for firms. However, the understanding of when and why consumers accept (reject) that firms collect information remains limited. We provide a better understanding of the privacy calculus, which is consumers' internal trade-off of the consequences of the collection, storage, and use of personal information. In addition to covering both positive and negative consequences we take into account that these consequences are not always certain to affect consumers. On the basis of this conceptualization, we develop the PRICAL index, which uses formative items to measure the privacy calculus. Following a qualitative phase, we empirically confirm the validity of these formative items (Study 1) and the index as a whole (Study 2). Besides being embedded in theory, the privacy calculus construct and the PRICAL index better explain behavioral intentions (Study 2) and actual behavior (Study 3) than currently used constructs, such as privacy concern and trust. We contribute by conceptualizing the privacy calculus, identifying the main (perceived) consequences of information collection, and developing an index (PRICAL) that explains when consumers accept (reject) information collection.

This paper is based on Beke, Frank T., Felix Eggers, Peter C. Verhoef, Jaap E. Wieringa (2017), "Consumers' Privacy Calculus: The PRICAL Index Development and Validation, working paper

## 3.1 Introduction

Over the past decade, as media exposure has raised consumers' awareness on the growing collection, storage, and use of information, privacy concerns have surged (Goldfarb and Tucker 2012; Rose, Rehse, and Röber 2012; TRUSTe 2016). Besides that neglecting these concerns could result in negative publicity, legislation in both the US and the EU compels firms to ask consumers permission to collect information. Moreover, the success of many new, data-driven products and services, such as fitness trackers and other '*smart*' devices, hinges on consumers' approval of information collection. Hence, a behavioral perspective may provide a fuller understanding of when and why consumers accept or reject that firms collect information about them (Bolton and Saxena-Iyer 2009; Rust and Huang 2014).

To understand when and why consumers accept or reject the collection, storage, and use of information, prior research in this area has focused primarily on privacy concern (Hong and Thong 2013; Malhotra, Kim, and Agarwal 2004; Smith, Milberg, and Burke 1996)[3]. However, consumers' behavior reflects a privacy paradox (John 2015), in that although privacy concern is on the rise, consumers are also disclosing more information than ever before. One reason for the discrepancy between privacy concern (an attitude) and information disclosure (a behavior) is that focusing on privacy concern (negative consequences) ignores the benefits (positive consequences) consumers enjoy from information collection. Therefore, following the field of information systems we measure consumers' privacy calculus, which we define as *consumers' internal trade-off of the negative and positive consequences of the collection, storage, and use of personal information* (Dinev and Hart 2006; Laufer and Wolfe 1977). Although several studies have empirically confirmed consumers trade off the positive and negative consequences of information collection, these studies either rely on ad-hoc developed measures that focus on a limited number of consequences (Mothersbaugh et al.

[3] Note that while measures for (e-)service quality (Parasuraman, Zeithaml, and Malhotra 2005; Wolfinbarger and Gilly 2003) include privacy, their main focus is on whether privacy is protected at a very generic level

2012; Xu et al. 2009; Zhao, Lu, and Gupta 2012) or study the antecedents without measuring the privacy calculus (Athey, Catalini, and Tucker 2017; Hann et al. 2007; Schumann, Von Wangenheim, and Groene 2014). As also stated in chapter 2, the fact that the privacy calculus has been neither conceptualized nor properly measured has curtailed the understanding of consumers' acceptance of information collection.

Our study contributes to the privacy literature in marketing in several ways. So far, the conceptualization of the potential consequences of the collection, storage, and use of customer information by firms has been rather limited. While privacy concern has been measured extensively, measures for the privacy calculus are yet to be developed and validated. In addressing this void, we conceptualize the privacy calculus and discuss in detail which types of consequences (dimensions) should be taken into account. Moreover, we develop and test the PRICAL index, which measures the privacy calculus using formative items, taking into account the valence and probability of the relevant consequences of the collection, storage, and use of information. Drawing on prior literature from both marketing and other domains (e.g., information systems) and a qualitative phase comprising interviews, we identify the consequences of the collection, storage, and use of information relevant from a consumer perspective. In addition to empirically validating the formative items (Study 1), we confirm the nomological validity of our PRICAL index, and we assure (incremental) predictive validity using both behavioral intentions (Study 2) and actual behavior (Study 3). By taking a broader perspective on the consequences of information collection, and looking beyond the negative side (privacy concern), the privacy calculus is better able to explain the acceptance or rejection of information collection than either privacy concern or trust. Our investigation shows that the frequently mentioned discrepancy between privacy concern and actual behavior—or the privacy paradox—occurs partially because of the use of limited measures for privacy concern.

## 3.2 Conceptual background

Rejecting or accepting information collection has mainly been explained by individuals' concerns about informational privacy (e.g., Smith, Milberg, and Burke 1996). However, collecting, storing, and using information also enables firms to better fulfill consumers' needs, for example via personalized products and services. Therefore, besides the negative consequences there are also positive consequences for consumers. The privacy calculus poses that consumers internally trade off the positive and negative consequences of firms' collection of personal information (Dinev and Hart 2006; Laufer and Wolfe 1977). In line with social exchange theory (Homans 1958; Premazzi et al. 2010), these consequences can be tangible or intangible (Acquisti, Taylor, and Wagman 2016), and consumers are affected by both the collection of information and the consequences that follow from the collection (Farrell 2012). Even though the privacy calculus is considered to be the most suitable framework for studying the acceptance of information collection (Acquisti, Brandimarte, and Loewenstein 2015; Culnan and Bies 2003), an extensive conceptualization of consumers' privacy calculus in the realm of their relationships with firms is still missing.

### *3.2.1 Consequences of information collection*

Every time consumers acquire a product or service from a firm, they engage in risk-taking behavior, as several potential consequences ('*risks*') might affect them. Prior work has shown that consumers consider different types of potential consequences, or risks (Bauer 1960), and risk was initially captured using five dimensions: performance, financial, psychological, social, and physical safety (Cunningham 1967). An additional dimension, time, was later added (Roselius 1971). These six dimensions capture a large portion of the variance in the overall risk of products and services, and are conceptually and empirically distinct (Jacoby and Kaplan 1972; Kaplan, Szybillo, and Jacoby 1974; Murray and Schlacter 1990; Stone and Grønhaug 1993). In addition to the negative uncertain consequences (risks) of products and

services these dimensions have also been used to capture positive uncertain consequences (rewards). Taking both positive and negative consequences (net return) into account explains consumers' preferences more fully (Peter and Ryan 1976; Peter and Tarpey 1975).

Consumers' acceptance of information collection can also be considered risk-taking behavior, with positive and negative consequences that can be immediate (e.g., monetary compensation for subscribing to a newsletter, or a feeling of discomfort) or more distant in time (e.g., better product recommendations, or possible theft of the information) (Acquisti, Taylor, and Wagman 2016). While prior work has hinted that consumers also consider different types of consequences when firms collect, store, and use information (e.g., White 2004; Stewart 2016; Milne et al. 2017), an exhaustive conceptualization of these consequences remains absent. We take a broad perspective on privacy by suggesting that consumers' privacy calculus can be conceptualized using these same risk-taking dimensions: performance, time, financial, psychological, social, and security.

*Performance risk.* The collection of information results in several consequences that affect the performance or quality of the products and services firms provide to consumers. The information enables firms to better understand the needs and preferences of consumers (Mithas, Krishnan, and Fornell 2005), and therefore possibly improve products and services in general (Slater and Narver 2000; Wedel and Kannan 2016). Moreover, as firms build detailed profiles about individual consumers, they are able to tailor their products and services, and their marketing communication, to individual consumers (Murthi and Sarkar 2003; Simonson 2005). While this could benefit consumers, opportunistic firms could also personalize in a way that serves the interest of firms rather than the interest of consumers (Frow et al. 2011; Hermalin and Katz 2006). For example, while differentiating products and services between valuable and less valuable consumers benefits the firm it could actually hurt less valuable consumers (Lacey, Suh, and Morgan 2007).

*Time risk.* Allowing firms to collect, store, and use consumers' information might reduce or increase the time consumers need to invest to interact or transact with firms. When firms retain consumers' payment details or re-use information to '*auto fill in*' forms, consumers might save time (Ackerman, Cranor, and Reagle 1999). Moreover, consumers might spend less time interacting with firms owing to an overall improvement of efficiency (Smith et al. 2014), or because consumers need less time to search for and find suitable products or services (Xu et al. 2011). However, allowing firms to collect information might also cost consumers more time. A relative minor issue could be that consumers have to invest time to provide additional information, for example to fill out forms. A more prominent issue is that once firms have collected information consumers might want to monitor how firms store and use their information to make sure that firms fulfill their promises.

*Financial risk.* When firms collect, store, and use information it could also result in monetary gains or losses for consumers. Insights drawn from personal information could increase firms' efficiency, and firms might pass on part of the monetary savings to consumers in the form of lower prices (Smith et al. 2014). More directly, information collection results in monetary savings for individual consumers via loyalty programs (Demoulin and Zidda 2009; Leenheer et al. 2007) or other monetary incentives (Acquisti, John, and Loewenstein 2013; Hann et al. 2007; Premazzi et al. 2010). In addition, firms' use of the information to adapt their prices to individual consumers could either hurt or benefit consumers (Acquisti and Varian 2005; Kannan and Kopalle 2001). Another potential financial consequence for consumers is the misuse of financial information, for example when additional money is charged from a consumer's account (Hille, Walsh, and Cleveland 2015).

*Psychological risk.* Firms' collection of information about consumers also affects how consumers feel about the firm, their privacy, and even themselves. In the context of privacy these psychological consequences are believed to be very important (Acquisti, Brandimarte,

and Loewenstein 2015). While a personalized experience might give consumers the feeling they are special to a firm (Hennig-Thurau, Gwinner, and Gremler 2002; Smith et al. 2014), reactance theory (Brehm 1966) suggests that information collection can also make consumers feel uncomfortable. Consumers might feel firms know too much about them, or that they lose control over their information (Hong and Thong 2013; Smith, Milberg, and Burke 1996). Moreover, consumers could perceive the collection of detailed information, with its accompanying loss of anonymity (White 2004), as intrusive (Aguirre et al. 2015; Goldfarb and Tucker 2011b). Likewise, when firms monitor consumers' behavior on a daily basis, consumers might perceive they are being watched (Smith et al. 2014).

*Social risk*. The collection, storage, and use of information could also affect consumers' interpersonal status or their relationships with friends and family. On the one hand, the collection of information could result in embarrassing disclosures (White 2004), as several recent high-profile examples have made painfully clear (e.g., Target revealing a customer's pregnancy). In addition, since privacy has become a widely debated topic, it has been suggested that consumers might suffer from having to explain or justify to their friends and family why they allow firms to collect their information (Goodwin 1991). On the other hand, the collection and distribution of information enables consumers to connect and interact with their social environment (Jiang, Heng, and Choi 2013; Lu, Tan, and Hui 2004; Zhao, Lu, and Gupta 2012). While online social networks exist by virtue of information collection, the ability to develop and maintain social relationships on such social networks can be considered a social consequence of information collection.

*Security risk*. Although the collection and storage of information has generally no influence on consumers' physical safety, there are potential consequences that relate to the safety (security) of consumers' information. As also discussed in chapter 1, security implies that consumers are protected from (unknown) outsiders illegally—that is, without proper

authorization—intercepting or accessing information (Belanger, Hiller, and Smith 2002), and is therefore not the equivalent of privacy. Still, these security-related consequences could matter to consumers' acceptance of firms collecting their information. As also captured by measures for privacy concern, consumers might experience situations in which unknown outsiders have access to their personal information (Smith, Milberg, and Burke 1996). More generally, when firms collect and store information, consumers become susceptible to flaws in the security of information systems (Hong and Thong 2013; Smith, Milberg, and Burke 1996). Therefore, given that information collection and storage results in consequences that affect the security of consumers' information, it might also affect the acceptance of information collection and thus the privacy calculus.

Given the wide variety of consequences, we conceptualize the privacy calculus as a multi-dimensional construct that consists of six dimensions. Together, these dimensions capture consumers' internal trade-off of the consequences of information collection, storage, and use. In Table 3-1 we define the dimensions in line with the general definition of the privacy calculus and provide a narrow overview of prior literature that has studied consequences related to these dimensions.

### *3.2.2 Contextual and individual differences*

Rather than looking at how consumers are affected when a firm collects information for a specific purpose, many studies have captured consumers' concerns about firms' privacy practices at a general level (Hong and Thong 2013; Malhotra, Kim, and Agarwal 2004; Smith, Milberg, and Burke 1996). Consumers' concerns and intentions on a general level are an unreliable predictor for actual behavior (e.g., Malhotra, Kim, and Agarwal 2004), as consumers' preferences with regard to privacy and information collection are context- and individual-specific (Nissenbaum 2004, 2011). Understanding the acceptance of information collection requires assessment of the perceived consequences (individual-specific) when a

**Table 3-1.** Definitions of dimensions

NOTE: All definitions start with "*The potential consequences for consumers resulting from the collection, storage, and use of information by firms that relate to …"*

| **Dimension** | **Definition** | **Based on** |
|---|---|---|
| Performance | *The quality of products or services, or the match between products and services and the needs of consumers.* | Frow et al. (2011); Lacey et al. (2007); Mithas et al. (2005); Simonson (2005); Wedel and Kannan (2016) |
| Time | *The amount of time or effort needed for consumers when dealing with the firm.* | Ackerman et al. (1999); Smith et al. (2014) |
| Financial | *The monetary gains and losses when dealing with the firm.* | Acquisti and Varian (2005); Hille et al. (2015); Premazzi et al. (2010) |
| Psychological | *Consumers' feelings with regard to the firm, their personal information, and their own lives in general.* | Edwards et al. (2002); Hong and Thong (2013); Smith et al. (1996); White (2004) |
| Social | *Consumers' interpersonal status and relationships with friends and family.* | Lu et al. (2004); Jiang et al. (2013); White (2004) |
| Security | *The unintended disclosure or exchange of information, or the unauthorized use of information by (unknown) third parties.* | Hong and Thong (2013); Malhotra et al. (2004); Smith et al. (1996); |

particular firm collects information for a specific purpose (context-specific). Thus, rather than looking at the objective benefits and costs one has to assess the context-specific subjective benefits and costs of information collection from the perspective of consumers (Acquisti, Taylor, and Wagman 2016). This subjectivity relates to whether consumers consider consequences as positive or negative—that is, the perceived valence of consequences. For example, while some consumers appreciate firms knowing their preferences and needs, other consumers might consider this knowledge as intrusive. Likewise, consumers might appreciate personalization from their regular firm but not from unknown firms (Bart et al. 2005), or only when the personalization is based on non-sensitive information (Mothersbaugh et al. 2012).

In addition to the perceived valence the consequences of information collection differ in their certainty of affecting consumers, for example because some consequences are more distant in time than others (Acquisti and Grossklags 2005b; Acquisti, Taylor, and Wagman 2016; Brandimarte, Acquisti, and Loewenstein 2013). Perceived risk theory (Bauer 1960; Conchar et al. 2004; Cunningham 1967) suggests taking into account the perceived probability that an outcome or consequence will occur. Understanding consumers' privacy calculus therefore requires correcting for the probability of consequences as perceived by consumers, as they might consider a potential loss to be severe (i.e., high concern) but also highly unlikely. Taking both contextual and personal differences into account, the privacy calculus depends on the context-specific, individually perceived valence and probability of the consequences of information collection, storage, and use. Although consumers might behave inconsistently with the actual consequences, we expect them to behave (more) in line with their context-specific, individual perceptions.

### 3.3 Index development

As shown in Figure 3-1, in developing a measure for the privacy calculus (PRICAL) we follow the most prevalent guidelines (Churchill Jr. 1979; MacKenzie, Podsakoff, and

Podsakoff 2011; Rossiter 2002). In line with our conceptualization, the privacy calculus is operationalized as *the consumer's perception of the valence and probability of performance, financial, psychological, social, time, and security consequences of firms' collecting, storing and using information about consumers, related to the products and services they acquire from that firm*. This definition implies that consumers rate the potential consequences of information collection, storage, and use on the basis of their perceived valence and probability, with each of these consequences belonging to one of the six dimensions. As our objective is to better understand how consumers respond when firms collect information, only consequences that affect a consumer or the relationship a consumer has with a particular firm are part of our operationalization of the privacy calculus. Moreover, while the privacy calculus is relevant in various contexts' each of these consequences should be specific enough so that together they explain the acceptance of information collection, storage, and use.

Consumers indicate whether they consider a consequence as positive, negative, or neutral on a bipolar scale aimed at measuring valence, which runs from very positive (+3) to very negative (-3). In addition, whether consumers consider a consequence as likely to affect them is measured on a unipolar scale for probability, which runs from very unlikely (1) to very likely (7). Multiplying the score on valence and probability for every consequence (Conchar et al. 2004; Peter and Tarpey 1975) ensures that consequences deemed neutral or unlikely have little influence. Summing the probability-weighted scores for each consequence within a dimension provides a value for each dimension, and summing the probability-weighted scores for each consequence across dimensions provides a '*privacy score*' for the entire privacy calculus. This privacy score can be used to predict beforehand whether consumers will accept or reject the collection, storage, and use of information or, more specifically, a data-driven product or service, whereby a positive (negative) privacy score suggests a consumer would accept (reject) the collection of personal information.

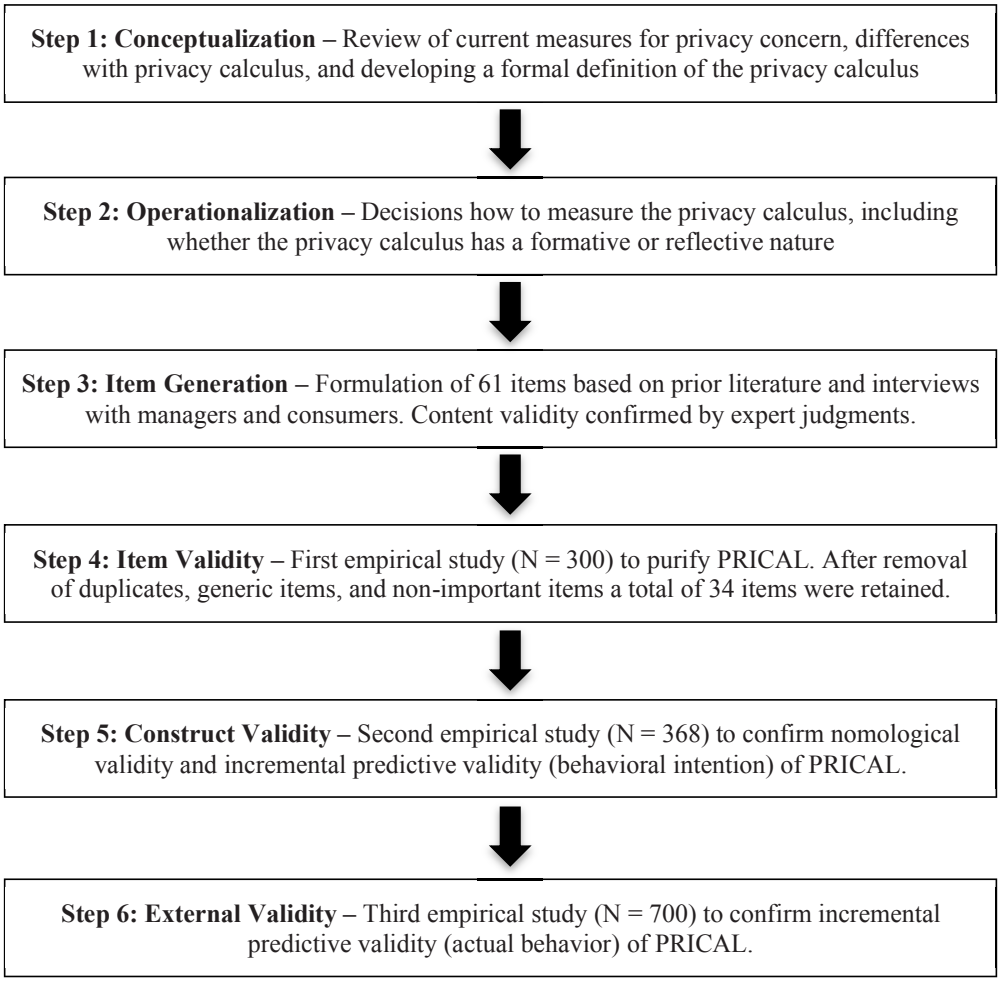



**Figure 3-1.** Overview of index development process

### *3.3.1 Formative construct*

The privacy calculus represents a consumer's mental calculation of the consequences of information collection, storage, and use (Pavlou 2011). As shown in Figure 3-2, the privacy calculus should therefore be considered a formative (latent) construct (Bollen and Lennox 1991), which should be measured using an index or composite (Diamantopoulos and Winklhofer 2001; Hair et al. 2017). Each underlying consequence (item) captures a unique element within a particular dimension, with all consequences within one dimension covering

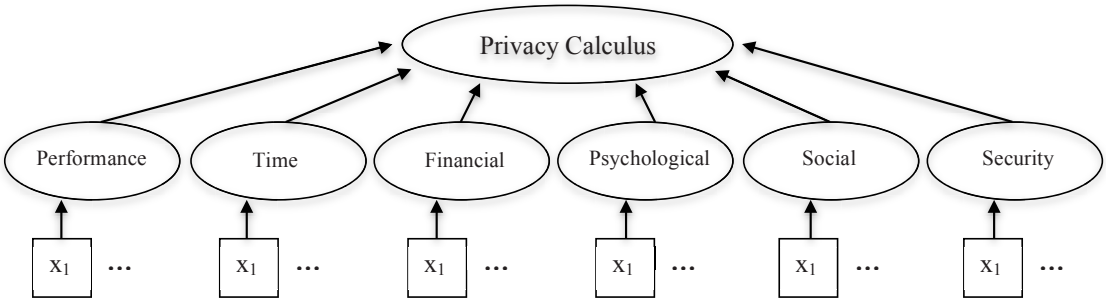



**Figure 3-2.** Privacy Calculus as a formative (latent) construct

an entire dimension, and all consequences together covering the entire privacy calculus construct. No reason exists to assume that the perceived consequences of information collection are related to each other or have to occur simultaneously, confirming the formative nature (Diamantopoulos and Winklhofer 2001; Jarvis, MacKenzie, and Podsakoff 2003). For formative constructs, each item is an essential part of the overall construct (Bollen and Lennox 1991; Diamantopoulos and Winklhofer 2001). Therefore, not only does the definition of the overarching construct and of each dimension determine which items should be included (Bagozzi 2011; Borsboom, Mellenbergh, and Van Heerden 2004), but the formative nature also affects how item validity should be assessed.

### *3.3.2 Item generation*

We developed an initial list of consequences of information collection, storage, and use aimed at covering all dimensions. While the dimensions and definitions are based on prior literature (Conchar et al. 2004; Kaplan, Szybillo, and Jacoby 1974), the initial list of items is based on qualitative interviews with managers and consumers from various industries, as well as on scientific and non-scientific literature (PwC 2014; Rose, Rehse, and Röber 2012; World Economic Forum 2014a). Every item aims to capture a unique consequence that is considered to be part of the internal trade-off consumers make with regard to the collection, storage, and use of information by firms. Given that we allow consumers to determine whether

consequences are positive or negative, all items are formulated to be as neutral as possible. After discussing whether the initial list included all relevant consequences (Hardesty and Bearden 2004; Rossiter 2002; Zaichkowsky 1985), we reformulated several items. A group of academic experts with the methodological background needed to understand the conceptual definition of each dimension rated whether the items were representative of the dimension, and therefore for the construct as a whole (MacKenzie, Podsakoff, and Podsakoff 2011; Rossiter 2002; Zaichkowsky 1985). Each of the resulting 61 items belonged to one of the six dimensions (see Appendix A for the initial list of items). Two convenience samples (N = 20, N = 26) confirmed the categorization of our items from a consumer's perspective, served as an initial test of whether the items were clear and understandable (Hinkin 1995), and confirmed that consumers could indicate the perceived valence and probability for each item.

### 3.4 Item purification – Study 1

We aimed to make the measurement tool more parsimonious by assessing the statistical validity of our items. Respondents were presented with one of three scenarios (retailer, telecom operator, or bank) in which a firm asked permission to collect information necessary for a data-driven offering, such as a personalized service or enhanced CRM program (see Appendix B for the scenarios). Given that we aim to explain consumers' acceptance of information collection by measuring consumers' privacy calculus we use willingness to accept that their information was collected (WTA) as the main dependent variable. While that suggests one could also measure WTA in order to predict consumers' acceptance of information collection, our main objective is explaining beforehand why consumers accept or reject information collection by measuring the privacy calculus, for which measuring WTA would be insufficient. Moreover, measuring consumers' privacy calculus would also provide more insight into why consumers accept (reject) information collection.

In the rest of the survey, we used the initial PRICAL index to measure the privacy calculus by deriving valence and probability sequentially for each item. Respondents first indicated the perceived valence of a consequence, immediately followed by the perceived probability of that same consequence. At the end of the survey we derived respondents' demographics and use of online services in general.

Besides that all scenarios were based on offerings from actual firms, we ensured external validity by using a firm with whom respondents had indicated they were actually transacting. To reduce the potential impact of (common) method bias we used several procedural remedies (MacKenzie and Podsakoff 2012; Podsakoff et al. 2003). By letting respondents first indicate their WTA we minimized the influence of implicit theories and the need for consistency Moreover, we allowed respondents to carefully read and process the items by presenting items in (random) groups of four on one page. By mixing the items across dimensions we aimed to diversify the survey, preventing respondents from filling out the same response for all items in one category (MacKenzie and Podsakoff 2012).

### *3.4.1 Sample*

We used an online research panel to invite respondents to our survey (MTurk, N = 300). Our sample contains slightly more males than females (56% vs. 44%) and had an average age of 37 (SD = 11.48), and most respondents had completed at least some type of college education (82%). After confirming all respondents completed the entire survey we checked our data for (common) method bias, which could still be an issue given the repetitive nature of our measure. Besides using Harman's Single-Factor Test (Podsakoff et al. 2003) we confirmed (common) method bias was not an issue by showing that removing the fastest respondents or respondents with the least variance in their answers had little influence on our results.

Hereafter, we continued to assess how consumers generally respond to the data-driven offering. While respondents had an average WTA of 3.4 on a scale from 1 to 7, the three

scenarios had significant differences between them ($F(1,299) = 7.140$, $p = 0.001$). This variation provides a good basis for testing the validity of the PRICAL index, which must be valid in each of these scenarios to be a widely applicable, generalizable measurement tool.

### *3.4.2 Item validity*

We used partial least squares (PLS) SEM to assess item validity, which is favored over covariance-based SEM when formative items are included (composite) and when the aim is to predict or explain a target variable as accurately as possible (Hair et al. 2017; Reinartz, Haenlein, and Henseler 2009). For our analyses, we used SmartPLS (Ringle, Wende, and Becker 2015), which determines significance of coefficients, weights, and loadings based on a bootstrapping procedure. When we needed to accommodate a higher-order construct, we used a repeated indicator approach to obtain parameter estimates (Hair et al. 2014).

Owing to the aforementioned theoretical differences between formative and reflective constructs, we assessed item validity using two criteria. First, we assessed the variance inflation factor (VIF) to identify items that correlate highly with multiple other items (Diamantopoulos and Winklhofer 2001). While internal consistency and unidimensionality are essential for reflective latent constructs (Diamantopoulos, Riefler, and Roth 2008; Diamantopoulos and Winklhofer 2001; Jarvis, MacKenzie, and Podsakoff 2003), formative constructs offer no reason to expect correlation between the items, as every item represents a different kind of consequence (Bollen 1984). In fact, correlated items make interpretation of the individual formative items more difficult, as correlation might result in unstable item weights that are insignificant or opposite to expectations (Cenfetelli and Bassellier 2009). As the guidelines regarding the height of VIF values remain contentious, we chose a pragmatic approach by first assessing the content validity of the item with the highest value (approximately 6), eventually working down to the lowest VIF value (approximately 1). Subsequently, we used the inter-item correlations to identify items that might be considered

duplicates or items that are overly generic in the perception of consumers, in that they represent the entire construct. Throughout this process of item purification, while we used the VIF values and the inter-item correlation as an indication for a lack of content validity, we only removed or changed items when it did not affect the conceptual domain of our construct (Bollen and Lennox 1991; Diamantopoulos, Riefler, and Roth 2008; Rossiter 2002).

In addition to assessing multicollinearity, we assessed the relative contribution of each item in explaining variance in the target dimension (Bollen 1984; Bollen and Lennox 1991). Items that have a low or insignificant relative contribution are potentially not an important part of an overall construct (Diamantopoulos, Riefler, and Roth 2008; Diamantopoulos and Winklhofer 2001; Jarvis, MacKenzie, and Podsakoff 2003). In case an item had a low relative contribution (weight) we assessed the absolute contribution of that item (loading) (Bollen and Lennox 1991; Cenfetelli and Bassellier 2009), as an item with a low relative contribution could still relate to the overall construct. This way we ensured that removing an item would not affect the conceptual domain (Diamantopoulos and Winklhofer 2001). Another indication for the importance of individual items, and thus for the inclusion or removal of items, is the extent to which they help in explaining our eventual target variable (WTA), as shown by the adjusted $R^2$ (Henseler, Ringle, and Sinkovics 2009). While removing any item with at least some variance will automatically decrease the amount of variance explained, a relatively minor decrease indicates the removed item hardly explains any additional variance in our target variable.

Besides assessing these criteria across all respondents, we also examined them for each scenario separately, since some items might be more relevant in one scenario (i.e., having a higher weight) than in other scenarios. Given our objective of explaining the acceptance of information collection in various contexts, retaining these items is crucial to

ensure content validity. Thus, we aimed to remove an item only when it was truly irrelevant, rather than removing an item that was of lesser relevance in one of the scenarios.

### *3.4.3 Results*

We conducted two rounds of item purification, focusing first on removing duplicates (multicollinearity) and subsequently on removing items that had a low contribution toward explaining the acceptance of information collection. Throughout both rounds, to ensure content validity we discussed extensively whether removing or reformulating items would affect the meaning of our construct.

On the basis of 14 items having a VIF values higher than 3, we concluded that several items suffered from multicollinearity (see Appendix A for the initial VIF values for all items). As shown in Table 3-2, the first round of item purification decreased the number of items from 61 to 43. While in some cases this process made clear that two or three items represented the same content, some items were too generic, resulting in a high correlation with up to 14 other items. Further, we reformulated several items as the inter-item correlations suggested they were either too similar within a dimension or too similar to items from another dimension. This similarity suggested they could be duplicates or were not a good representation of the dimension the item should represent.

In the second round we further decreased the number of items from 43 to 34 (Table 3-2), as we focused on the relative contribution of each remaining item (indicator weights) and the extent to which each item related to the overall privacy calculus. These weights were used as guidance, because to ensure content validity some items were retained despite insignificant weights. Moreover, we also critically assessed whether insignificant weights or weights opposite to bivariate correlations (loadings) were caused by remaining multicollinearity (Cenfetelli and Bassellier 2009), although our first round of item purification resolved most issues related to multicollinearity (as illustrated by lower VIF values).

**Table 3-2.** Overview item purification – Study 1

| | **Round 1** | **Round 2** |
|---|---|---|
| Main focus | Removing duplicate items | Removing less important items |
| Criteria | Multicollinearity (VIF, correlations) | Relative contribution (weights, loadings) |
| Change in number of items | 61 items (old) → 43 items (new) | 43 items (old) → 34 items (new) |
| Change in adjusted $R^2$ | 0.555 (old) → 0.542 (new) | 0.542 (old) → 0.544 (new) |

In summary, based on two rounds of item purification we decreased the number of items from 61 to 34, with each dimension being represented by at least four items. For formative constructs it is crucial to ensure that removing items does not infringe content validity (Bollen and Lennox 1991; Diamantopoulos, Riefler, and Roth 2008; Rossiter 2002). Removing nearly half of the original items is warranted here as many of these items captured the same content. This is also supported by the fact that item purification only slightly decreased the adjusted $R^2$ (from 0.555 to 0.543). Therefore, the items we removed were less important in explaining the willingness to accept information collection.

## 3.5 Construct validity – Study 2

After confirming item validity, we conducted a second study using an online research panel from the Netherlands to ensure the validity of the PRICAL index as a whole. As depicted in Figure 3-3, we included other constructs that theoretically should relate to the privacy calculus (nomological validity), and '*rival*' constructs that have been used previously to explain the acceptance of information collection (predictive validity) (Diamantopoulos, Riefler, and Roth 2008; Jarvis, MacKenzie, and Podsakoff 2003). With regard to nomological

validity, we included constructs related to the consumer (privacy violation experience, personality), to the firm or context (information sensitivity), and to the relationship between the firm and consumer (behavioral loyalty). Moreover, we assessed the incremental predictive validity by comparing the PRICAL index with measures for privacy concern and trust.

*Privacy violation experience*

Consumers who have directly experienced an (negative) outcome of their behavior usually also have a stronger (negative) attitude towards that behavior (Fazio, Powell, and Williams 1989). Also in the context of privacy consumers who have experienced a privacy violation, either directly or indirectly, are more concerned about their privacy (Bansal, Zahedi, and Gefen 2015; Malhotra, Kim, and Agarwal 2004; Smith, Milberg, and Burke 1996). We expect a similar learning effect with respect to the privacy calculus, in the sense that consumers who have experienced a privacy violation more (less) often have a more negative (positive) privacy calculus.

$H_1$: Privacy violation experience is negatively related to the privacy calculus.

*Personality*

Moreover, we expect the privacy calculus to also be related to consumers' personality. With regard to the '*big five*' personality traits (McCrae and Costa Jr. 1987) agreeableness has been linked to a lower privacy concern (Junglas, Johnson, and Spitzmüller 2008) and a higher acceptance of new technologies (Devaraj, Easley, and Crant 2008). Consumers high on agreeableness are cooperative, not very skeptical, and more likely to agree (McCrae and Costa Jr. 1987). Therefore, we also expect that agreeable consumers are less skeptical about information collection, which should reflect in a more positive privacy calculus.

$H_{2a}$: Agreeableness is positively related to the privacy calculus.

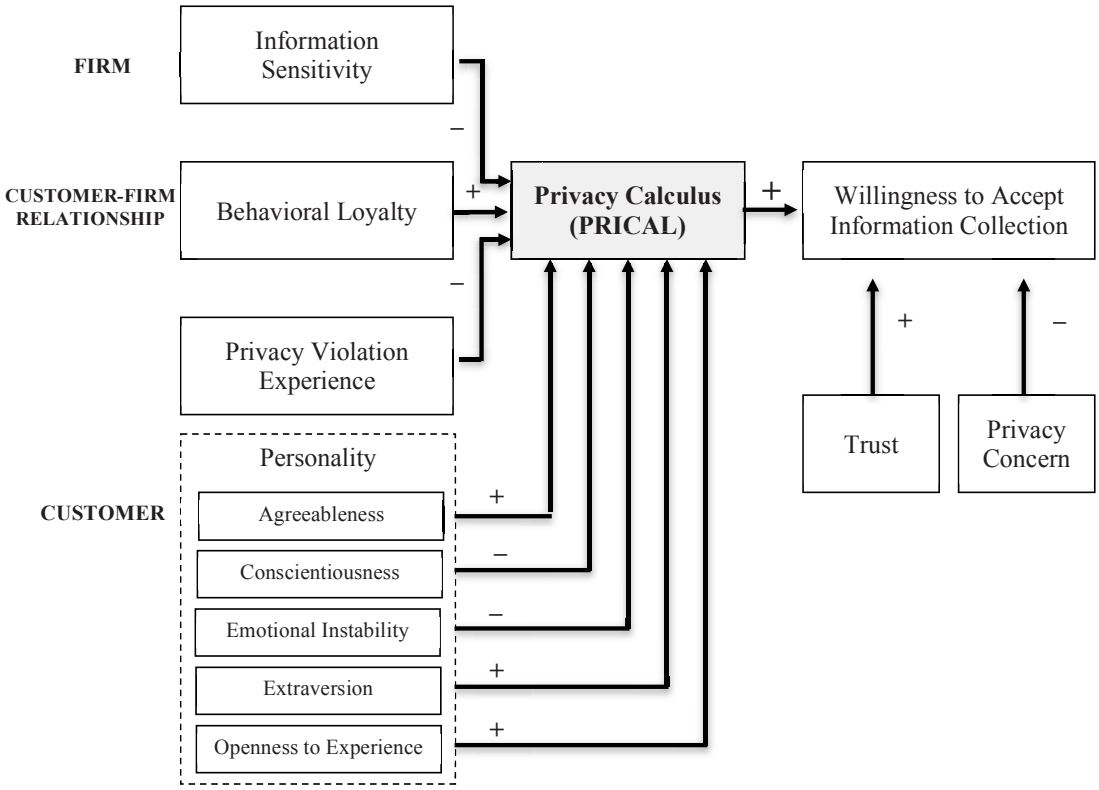



**Figure 3-3.** Overview of nomological network

Conscientiousness represents to what extent someone is self-disciplined and careful (McCrae and Costa Jr. 1987). Therefore, conscientious consumers are generally more concerned about their privacy (Junglas, Johnson, and Spitzmüller 2008) and see more risks with regard to privacy (Bansal, Zahedi, and Gefen 2010). We expect consumers high on conscientiousness to be more vigilant, and thus to consider negative consequences as more likely. As result, consumers high on conscientiousness should have a more negative privacy calculus than consumers low on conscientiousness.

$H_{2b}$: Conscientiousness is negatively related to the privacy calculus.

Emotional instability, or neuroticism, refers to the extent to which consumers feel insecure and how they cope with stress (McCrae and Costa Jr. 1987). Prior studies show that emotional instability is positively related to privacy-risk beliefs (Bansal, Zahedi, and Gefen 2010) and privacy concern (Bansal, Zahedi, and Gefen 2015) and negatively related to technology acceptance (Devaraj, Easley, and Crant 2008), and that emotional instable people are more likely to protect their privacy (Korzaan and Boswell 2008). We expect that emotionally unstable consumers are more anxious about information collection, and therefore consider the potential negative consequences more likely. Given that we also believe that these consumers are less secure about any potential positive consequences, we expect that emotional instability relates negatively to the privacy calculus.

$H_{2c}$: Emotional instability is negatively related to the privacy calculus.

Extraversion refers to being talkative, social, and generally more outgoing (McCrae and Costa Jr. 1987). Extraverted people are less concerned about exposing information to others, and extraversion relates negatively to privacy risk beliefs (Bansal, Zahedi, and Gefen 2010) and positively to technology acceptance (Devaraj, Easley, and Crant 2008). Extraverted consumers should be less tentative in sharing information about themselves since they should consider information disclosure not necessarily as a negative consequence. Therefore, we expect extraversion to relate positively to the privacy calculus.

$H_{2d}$: Extraversion is positively related to the privacy calculus.

People high on openness to experience tend to be more imaginative and daring (McCrae and Costa Jr. 1987), to regard innovation more positively (Marcati, Guido, and Peluso 2008), and more inclined to accept new technologies (Devaraj, Easley, and Crant 2008). These consumers should therefore also be more interested in the potentially positive

consequences of information disclosure, suggesting that openness to experience relates positively to the privacy calculus.

$H_{2e}$: Openness to experience is positively related to the privacy calculus.

*Information sensitivity*

Consumers are affected by the type of information (Acquisti, John, and Loewenstein 2012), and consider financial and medical information to be more sensitive than information about online behavior and habits (Phelps, Nowak, and Ferrell 2000). Information sensitivity should make the potential negative consequences more negative, while also decreasing the appeal of the potential positive consequences. For example, while receiving personalized advertisements might be considered positive, consumers would most likely oppose such personalization when it relates to '*sensitive*' information about them (White 2004). Therefore, we expect that information sensitivity relates to the privacy calculus, in the sense that when firms want to collect sensitive information consumers' privacy calculus is more negative.

$H_3$: Information sensitivity is negatively related to the privacy calculus.

*Behavioral loyalty*

When consumers have been affiliated with a particular firm for a long time (behavioral loyalty), they are generally confident that the firm acts in their best interest and thus will not harm them (Dick and Basu 1994). Therefore, the probability for negative consequences (risks) should be lower and the privacy calculus more positive. Moreover, as they are also more likely to expect the firm to provide them with beneficial products and services (Kim, Ferrin, and Rao 2009), consumers will probably hold similar expectations for benefits related to information collection. Therefore, we expect that behavioral loyalty is positively related to the privacy calculus.

$H_4$: Behavioral loyalty is positively related to the privacy calculus.

*Privacy concern and trust*

The acceptance of information collection has most often been explained using two alternative constructs. First, as previously stated, many studies have used privacy concern to explain the acceptance of information collection. The most widely used measurement tool measures consumers' concern about information practices based on four reflective dimensions: collection, unauthorized secondary use, improper access, and errors (Smith, Milberg, and Burke 1996). Given that these dimensions focus on information practices in general, we chose to adapt the measurement tool to better represent the specific context of our study. Moreover, as a robustness check, we also include a more recent, abbreviated scale to measure privacy concern (Dinev and Hart 2006)

Besides privacy concern, the acceptance of information collection has also been explained by trust (Premazzi et al. 2010). Trust has been conceptualized and operationalized in many ways, and we include a well established, multi-dimensional measurement tool for trust (McKnight, Choudhury, and Kacmar 2002), which captures trust based on three reflective dimensions: benevolence, integrity, and competence. Besides, we also include a more condensed scale for trust as robustness check (Mothersbaugh et al. 2012). To confirm incremental predictive validity, the privacy calculus should be more closely related to the acceptance of information collection than privacy concern and trust.

> $H_5$: The privacy calculus explains more variance in the willingness to accept information collection compared to (a) privacy concern and (b) trust.

### *3.5.1 Design and sample*

Once again we presented respondents with a scenario (telecom operator, insurance company[4]) in which a firm they transacted with asked permission to collect information necessary for a

[4] We also included a social media scenario that was based on actual use rather than intentions. Because the respondents did not show variation in their use behavior, i.e., every respondent made use of social media, we discarded this scenario from the analysis.

data-driven offering (see Appendix C for the scenarios). Other than containing the additional constructs (see Appendix D for an overview of the measurement items of the additional constructs), the set-up of the second study and the procedural remedies to reduce the potential impact of (common) method bias were similar to study 1 (MacKenzie and Podsakoff 2012; Podsakoff et al. 2003). After reading the scenario, the respondents first had to indicate their WTA before disclosing their perceptions. The main difference from study 1 was that in this second survey the items for the PRICAL index were presented in groups of five. More specifically, we first derived the perceived valence for five items, followed by the perceived probability for these same items on the next page. To supplement the demographic information provided by the research panel agency, we obtained some additional information about our sample at the end of the survey.

Our sample consisted of slightly more males than females (51.5% vs. 48.5%), was relatively balanced in terms of age (<30 years: 16.5%; 30-39: 14.3%; 40-49: 20.3%; 50-59: 19.3%; >60: 29.5%), had an average education, and overall was representative of the Dutch population. After confirming all respondents completed the entire survey we checked our data for outliers and (common) method bias. We removed 32 respondents that could be considered '*straight-liners*'—that is, respondents for which the variance in answers was below 0.5. We used the remaining sample (N = 368) to assess nomological and predictive validity. Moreover, besides using Harman's Single-Factor Test to test for (common) method bias (Podsakoff et al. 2003) we confirmed throughout our analysis that removing the fastest respondents or respondents with the least variance in their answers had no further influence on our results.

### *3.5.3 Results*

Following the confirmation of the validity of the other multi-item measurement tools (see Appendix D for Cronbach's α), we used SmartPLS (Ringle, Wende, and Becker 2015) to

re-confirm the validity of items of the PRICAL index. Thereafter, we confirmed discriminant validity by confirming that the item-to-item correlations within the privacy calculus were higher than the item-to-item correlations with items from constructs other than the privacy calculus (Klein and Rai 2009). In addition, bivariate correlations confirmed that the privacy calculus is related, but not completely identical, to privacy concern ($\rho$ = -0.372) and trust ($\rho$ = 0.476) (Gerbing and Anderson 1988; MacKenzie, Podsakoff, and Podsakoff 2011). Finally, in line with recent guidelines with regard to formative constructs (Diamantopoulos and Winklhofer 2001; Jarvis, MacKenzie, and Podsakoff 2003) we used simple correlations based on summated scores (Nunnally and Bernstein 1994) to assess nomological and predictive validity. In addition, we assessed nomological and predictive validity using PLS-SEM by applying a two-step approach, in which we first calculated the latent variable scores for our latent variables to test our nomological network (Hair et al. 2014).

*Nomological validity.* As Table 3-3 shows, the bivariate correlations and coefficients from PLS-SEM are in line with most of our hypotheses. These results are consistent across scenarios, and the coefficients are robust for changes in the nomological network (Cenfetelli and Bassellier 2009; Nunnally and Bernstein 1994). Despite that having directly experienced more privacy violations is unrelated to the privacy calculus ($\beta$ = 0.018, $p$ = 0.752), this is mainly because the majority of our sample (54%) had never experienced a privacy violation. The number of consumers who had never heard of a privacy violation was much smaller (14.7%), and the number of indirect privacy violations is significantly negatively related to the privacy calculus on a 10% level ($\beta$ = -0.117, $p$ = 0.052).[5]

[5] Recoding direct and indirect privacy violation experience into binary variables (0 = never, 1 = at least once) shows that the privacy calculus is more negative for consumers that have a privacy violation experience (direct: $\mu$ = -65.42, indirect: $\mu$ = -48.15) compared to consumers who have never had that experience (direct: $\mu$ = -95.03, indirect: $\mu$ = -84.23), although the difference is only marginally significant (direct: privacy calculus (366) = 1.938, $p$ = 0.053, indirect: privacy calculus (366) = 2.808, $p$ = 0.095).

**Table 3-3.** Nomological validity – Study 2

| **Hypotheses** | **ρ** | **β** | **Supported?** |
|---|---|---|---|
| $H_1$: Privacy violation experience → PRICAL (–) | | | |
| - Direct | -0.091$^{ns}$ | 0.018$^{ns}$ | Partly |
| - Indirect | -0.168** | -0.117$^{+}$ | |
| $H_{2a}$: Agreeableness → PRICAL (+) | 0.148** | 0.139* | Yes |
| $H_{2b}$: Conscientiousness → PRICAL (–) | -0.122** | -0.154* | Yes |
| $H_{2c}$: Emotional instability → PRICAL (–) | -0.082$^{ns}$ | -0.044$^{ns}$ | No |
| $H_{2d}$: Extraversion → PRICAL (+) | 0.253** | 0.207** | Yes |
| $H_{2e}$: Openness to experience → PRICAL (+) | 0.133** | -0.011$^{ns}$ | Partly |
| $H_3$: Information sensitivity → PRICAL (–) | -0.367** | -0.367** | Yes |
| $H_4$: Behavioral loyalty → PRICAL (+) | 0.005$^{ns}$ | -0.002$^{ns}$ | No |

$^{**}p < 0.01$ $^{*}p < 0.05$ $^{+}p < 0.10$

The relationship between consumers' personality[6] and their privacy calculus is for the most part consistent with our expectations. First, consumers high on agreeableness, who are less skeptical of innovations and are more cooperative, have a more positive privacy calculus (β = 0.139, $p$ = 0.023). Furthermore, when consumers score high on conscientiousness their privacy calculus becomes more negative (β = -0.154, $p$ = 0.016). Conscientiousness implies that consumers put more thought into their decisions, and thus consider the risks of information collection to be greater. In addition, extraversion is positively related to the privacy calculus (β = 0.207, $p < 0.001$). Extraversion implies that someone is outgoing and

[6] As the consistency between the items for each personality trait was low each personality is represented by one item that best represents the content of the personality trait.

wants to be noticed. Therefore, extraverted consumers are less hesitant to disclose information about themselves to firms. Moreover, although emotional instability was not significantly related to the privacy calculus ($\beta = 0.044$, $p = 0.443$), the signs of both the correlation and the coefficient pointed in the right direction, providing some support for our hypotheses. Finally, while the coefficient for openness to experience is not significant ($\beta = -0.011$, $p = 0.858$), the bivariate correlation did support our hypothesis that when consumers are more open to experience their privacy calculus becomes more positive.

The privacy calculus relates not only to differences between consumers but also to differences between firms. In line with our expectations, the privacy calculus is more negative when consumers consider the information firms collect as sensitive ($\beta = -0.367$, $p < 0.001$). However, the privacy calculus is not significantly related to behavioral loyalty ($\beta = -0.002$, $p = 0.965$), suggesting that the number of years a customer is loyal to a firm is unrelated to the perceived valence and probability of the consequences of information collection. Apparently, being customer for a long time does not necessarily imply that you expect less negative or even positive consequences.

In summary, although two constructs (behavioral loyalty and emotional instability) were unrelated to the privacy calculus, we confirm the majority of our nomological network. Therefore, we conclude that nomological validity of our PRICAL index is assured.

*Predictive validity.* Table 3-4 indicates that the privacy calculus is more consistently related to consumers' willingness to accept information collection (WTA) than privacy concern or trust (Nunnally and Bernstein 1994). The bivariate correlation of the summated scores for the privacy calculus and consumers' WTA is significantly larger than the correlation between WTA and privacy concern ($Z = 4.33$, $p < 0.000$) or trust ($Z = 4.68$, $p < 0.000$). Likewise, the privacy calculus explains more variance (36.7%) than privacy concern (7.4%) and trust (12.2%) when regressing WTA on each construct with control variables.

**Table 3-4.** Predictive validity – Study 2

| Willingness to accept | Correlation ρ | OLS Adj.$R^2$ | PLS-SEM Adj.$R^2$ |
|---|---|---|---|
| Privacy calculus *(our study)* | 0.603** | 0.367 | 0.378 |
| Privacy concern *(Smith et al. 1996)* | -0.359** | 0.074 | 0.006 |
| Trust *(McKnight et al. 2002)* | 0.336** | 0.122 | 0.003 |

$^{**}p < 0.01$ $^{*}p < 0.05$ $^{+}p < 0.10$

While these results are based on a summated approach, which assumes equal importance of all items and dimensions, Table 3-4 shows that also when the impact of every individual item is weighed using PLS-SEM (Henseler et al. 2014), the privacy calculus explains more variance (adjusted $R^2$) in consumers' willingness to accept than privacy concern and trust. These results also hold when using alternative measures for privacy concern (Dinev and Hart 2006) or trust (Mothersbaugh et al. 2012), and are not driven by the choice of measurement model (formative vs. reflective) (Klein and Rai 2009). Therefore, we accept $H_5$ and state that the privacy calculus explains more variance in the willingness to accept information collection than privacy concern and trust.

### 3.6 External validity – Study 3

The privacy paradox refers not only to the aforementioned discrepancy between attitudes (privacy concern) and behavior, but also to a discrepancy between behavioral intentions and actual behavior with regard to privacy (Norberg, Horne, and Horne 2007). To confirm predictive validity based on actual behavior, we linked the privacy calculus to an actual decision regarding the acceptance of information collection. For this we cooperated with a Dutch insurance company that planned to introduce a new type of car insurance that is based on collecting information about consumers' driving behavior (usage-based insurance, UBI).

Customers of the insurance firm were invited to participate in a pilot study that required them to fill out a survey containing the PRICAL index and several other constructs before the introduction of the car insurance. Non-accepters, i.e., customers who rejected information collection, filled out a comparable survey. The set-up of the survey was similar to the survey in study 1, as respondents first indicated the perceived valence of a consequence, immediately followed by the perceived probability of that same consequence (see Appendix D for an overview of the measurement items of the additional constructs). The procedural remedies to reduce the potential impact of (common) method bias were similar to both prior studies (MacKenzie and Podsakoff 2012; Podsakoff et al. 2003),

### *3.6.1 Sample*

In all, 699 customers were willing to switch to usage-based insurance, of which 616 respondents filled out the survey. Of the customers who refused to switch, 225 were initially willing to fill out the survey, with 84 respondents completing the entire survey. Thus, in total our sample consisted of 700 respondents (616 accepters, 84 non-accepters). We confirmed (common) method bias was not an issue in a similar manner as study 1 and 2 (Harman's Single-Factor Test, comparison of samples).

Subsequently, we continued to assess to what extent the PRICAL index could explain the acceptance of information collection—that is, the decision to adopt UBI from this insurance company. Before this, we used a standard Heckman two-step approach to assess whether opening the e-mail containing the invitation results in sample selection bias (Heckman 1979). Since the inverse Mills' ratio was not significantly related to the acceptance of information collection, we present our results without correction in Table 3-5. Besides ruling out the sample selection bias, we assessed the influence of how the privacy calculus is measured. Measuring valence and probability in reverse order for half of the sample in a follow-up survey, completed by a subset of our sample (N = 318), confirmed the absence of a

significant difference in the privacy calculus based on the order of measuring valence and probability (privacy calculus (318) = 1.685, $p < 0.093$).

### *3.6.2 Results*

After confirming the validity of the other multi-item measurement tools (see Appendix D for Cronbach's α), we used SmartPLS (Ringle, Wende, and Becker 2015) to re-confirm the validity of items of the PRICAL index. Thereafter, we used a summated version of the PRICAL index (and rival constructs) to assess how well it predicts the acceptance of information collection beforehand. We confirmed that the mean values for the privacy calculus were consistent with the acceptance of information collection, i.e., the PRICAL index for accepters was on average positive (μ = 57.68, sd = 95.354), whereas the PRICAL index was on average negative for non-accepters (μ = -132.08, sd = 130.980). An independent samples t-test confirmed the significance of this difference (privacy calculus (95.363) = -12.823, $p < 0.0001$). Moreover, we confirmed that on an individual consumer level the majority of the accepters had a positive privacy calculus (458 out of 616, 74%), whereas the majority of non-accepters had a negative privacy calculus (74 out of 84, 88%).

As depicted in Table 3-5, we used a simple binary logistic regression to confirm incremental predictive validity. In addition to a model with only control variables (model 1), we compared the incremental predictive validity of trust (model 2), privacy concern (model 3), trust and privacy concern (model 4), and the privacy calculus (model 5). Comparison of the relationship between the acceptance of information collection and the privacy calculus with the relationship between acceptance of information collection and privacy concern or trust showed that all three constructs are significantly related to the acceptance of information collection. However, model fit (-2LL, AIC, Nagelkerke $R^2$) indicates that the privacy calculus is best at explaining the acceptance of information collection.

**Table 3-5.** Acceptance of information collection (binary logit) – Study 3

| | Model 1 | Model 2 | Model 3 | Model 4 | Model 5 |
|---|---|---|---|---|---|
| **Predictor** | **β** | **β** | **β** | **β** | **β** |
| Constant | 0.322 | -0.843 | 5.791 | 4.641 | 4.134 |
| Trust | - | 0.532** | - | 0.339** | - |
| Privacy concern | - | - | -1.080** | -0.980** | - |
| Privacy calculus | - | - | - | - | 0.019** |
| *Controls* | | | | | |
| Innovativeness | 0.275** | 0.266** | 0.363** | 0.356** | 0.365** |
| Involvement | 0.226 | 0.051 | 0.248+ | 0.142 | -0.116 |
| Number of products | 0.026 | -0.005 | -0.046 | -0.069 | -0.083 |
| Years customer | -0.006 | -0.005 | 0.003 | 0.007 | 0.035 |
| Age | -0.019+ | -0.027* | -0.029* | -0.037** | -0.059** |
| -2LL | 470.148 | 437.190 | 364.599 | 354.890 | 275.145 |
| AIC | 482.148 | 451.190 | 378.599 | 370.890 | 289.145 |
| Nagelkerke-$R^2$ | 0.071 | 0.160 | 0.341 | 0.363 | 0.538 |

**$p < 0.01$ * $p < 0.05$ + $p < 0.10$

Given the size of our sample, creating a hold-out sample is not feasible. However, Table 3-6 shows that when looking at the within-sample classification only the privacy calculus is able to correctly classify non-accepters as non-accepters, as both trust and privacy concern classified all respondents as accepters.

**Table 3-6.** Within-sample classification – Study 3

| Observed / Predicted | PRICAL | Trust | Privacy concern |
|---|---|---|---|
| Accept / Accept* | 608 | 616 | 616 |
| Accept / Not Accept | 8 | 0 | 0 |
| Not Accept / Not Accept* | 39 | 0 | 0 |
| Not Accept / Accept | 45 | 84 | 84 |

** Correct classification*

| % correct | PRICAL | Trust | Privacy concern |
|---|---|---|---|
| Accept | 98.7% | 100% | 100% |
| Not Accept | 46.4% | 0% | 0% |
| Total | 92.4% | 88% | 88% |

## 3.7 Discussion

Firms' growing reliance on consumers' approval of information collection, has made it imperative to understand and predict beforehand when and why consumers accept the collection, storage, and use of personal information. While the privacy paradox suggests that consumers are unaffected by their attitudes (i.e., privacy concern), we believe this discrepancy is predominantly due to the omission of positive consequences. Consumers not only focus on the negative consequences, but internally trade off these '*costs*' against the benefits of information collection. Moreover, as these consequences are not always immediate, measurement of consumers' privacy calculus must take into account the perceived probability in addition to the perceived valence. In this study we develop the PRICAL index to measure the privacy calculus, taking into consideration both benefits and costs of products and services that are contingent on information collection.

We consider the privacy calculus a formative construct, which we measure using a multi-dimensional index consisting of 34 items that measure six conceptually distinct dimensions. As the (potential) consequences of information collection vary widely, all items depicted in Table 3-7 are needed to understand consumers' privacy calculus across various contexts. Even when certain items or consequences seem less relevant in certain contexts', correcting for the perceived probability accounts for this.

As a whole, the PRICAL index explains a substantial amount of variance in the acceptance of information collection. More specifically, it explains consumers' willingness to let a bank collect and use detailed payment information (Study 1: 70.5%) and consumers' acceptance of the collection of information on their purchases by an offline retailer (Study 1: 67.2%). In addition, the PRICAL index explains a large part of the variance in consumers' willingness to let a telecom provider collect information about their location (Study 1: 42%, Study 2: 57.6%) and their willingness to allow an insurance company to collect driving behavior (Study 2: 43.5%). Besides explaining these behavioral intentions, the PRICAL index also explains consumers' actual acceptance of information collection (behavior). When looking at a summated PRICAL index for each consumer, the majority of accepters of information collection had a positive privacy calculus, while most consumers who reject information collection had a negative privacy calculus. Despite the fact that part of the acceptance remains unexplained for various reasons (e.g., irrationality), we demonstrate that the PRICAL index explains the acceptance of information collection rather well.

**Table 3-7.** Item list – PRICAL Index

NOTE: All items start with *"When [Your Firm] collects information about me …"*

| **Financial** |
|---|
| … I receive monetary compensation. |
| … I have access to monetary savings (i.e., discounts). |
| … [Your Firm] is able to keep their prices low (e.g., due to more efficiency, customer insights). |
| … [Your Firm] adapts its prices to my personal profile. |
| … [Your Firm] is able to generate additional revenues. |
| … [Your Firm] charges additional money from my credit card or bankcard. |

| **Performance** |
|---|
| … products and/or services of [Your Firm] are adapted to my personal preferences. |
| … I am denied certain services and/or products. |
| … [Your Firm] makes fewer errors when I interact or transact with them. |
| … I receive better service than other customers. |
| … I receive information or feedback giving insight in my own behavior or decisions. |
| … I have access to free (additional) services or content. |
| … I receive communication (e.g., advertisements) that is tailored to my personal needs or preferences. |

| **Psychological** |
|---|
| … it feels like [Your Firm] knows a lot about me. |
| … it feels like [Your Firm] follows my behavior. |
| … it feels like [Your Firm] controls the collection, storage, and use of my personal information. |
| … my relationship with [Your Firm] becomes closer. |
| … [Your Firm] makes me feel special. |
| … I have the possibility to express myself. |

NOTE: All items start with *"When [Your Firm] collects information about me ..."*

| **Social** |
|---|
| … I can connect with friends and family. |
| … I have to explain to my family and friends why I shared personal information. |
| … my family and friends receive communication (e.g. advertisements) that is adapted to my personal needs. |
| … family and friends become aware which products or services I am interested in. |

| **Security** |
|---|
| … my personal information ends up with other firms or organizations. |
| … my personal information will be used for (identity) fraud. |
| … my personal information will become (accidently) publicly available. |
| ... it depends on the stability of information systems whether my information is kept safe. |
| … my personal information is visible for other people, like employees. |
| … I receive unrequested communication. |

| **Time** |
|---|
| … I can find the right product or service faster. |
| … the process of completing transaction is (partly) automated. |
| … I have to actively provide additional information (e.g., via forms). |
| … I have to take the time to protect my (online) identity. |
| … I have to take the time to monitor how [Your Firm] handles my information. |

In terms of incremental predictive validity, the PRICAL index better explains the willingness to accept information collection than consumers' privacy concern (Smith, Milberg, and Burke 1996) or their trust in a specific firm (McKnight, Choudhury, and Kacmar 2002). Moreover, with respect to the actual acceptance of information collection the PRICAL index better differentiates between consumers who accept or reject information collection than privacy concern or trust in a firm. In particular, the PRICAL index is at least somewhat able to classify non-accepters as such, while both privacy concern (Dinev and Hart 2006) and trust (Morgan and Hunt 1994) were unable to do so.

### 3.8 Limitations and future research

Although the PRICAL index predicts (and explains) the acceptance of information collection, correspondence to behavior can only be expected when consumers are conscious they are making a decision about the collection of information. Thus, when consumers are unaware they have a choice or when information is being collected without consumers realizing this, their privacy score and their actual behavior could differ. Nevertheless, our measure for the privacy calculus is widely applicable, as we have used a wide variety of contexts throughout the process of developing the PRICAL index. Future research could expand the applicability of our measure by testing it in more contexts, for example focusing more on products and services that rely on information collection but provide a direct monetary compensation as well, such as loyalty programs.

Given our focus on conceptualizing the privacy calculus, and developing and validating the PRICAL index we do not discuss the influence of every dimension in detail. Although all dimensions were individually positively related to the acceptance of information collection, future research could assess the extent to which the importance of dimensions differs for specific context. Besides providing firms a better understanding on which dimension to focus (e.g., in their communication, Conchar et al. 2004), it would also reveal

whether for the calculation of the overall PRICAL index the differences between the importance of these dimensions should be taken into account. Future research should focus on the step of determining norms (Churchill Jr. 1979) or enumeration (Rossiter 2011).

Besides testing and applying the PRICAL index in more contexts, future research could also try to assess whether cultural differences between countries have any influence. Findings could be important given that cross-national differences exist in privacy regulation (Holtrop et al. 2017). Another avenue for future research would be to understand how the privacy calculus could be influenced. What is the role of firms' privacy policies and communication? How do external events and media coverage affect the privacy calculus and its underlying dimensions?

## 3.9 Conclusion

In sum, we provide a better understanding of the privacy trade-off consumers make with regard to their relationship with firms. Besides identifying the main perceived consequences of information collection, both positive and negative, we use these consequences to develop an index that can measure consumers' privacy calculus. The PRICAL index not only explains beforehand when consumers will accept (reject) information collection, but also why consumers accept (reject) information collection. As the importance of information grows, and firms are forced to ask for permission to collect information, understanding consumers' approval of information collection, storage, and use becomes crucial.

# Chapter 4

# Promoting Privacy: How Consumers Trade Off Privacy Elements


**Abstract**

Privacy has received growing attention from consumers in recent years. We suggest that this attention can represent an opportunity for firms that optimize their privacy strategy. In order to differentiate from competitors, firms could actively promote privacy practices that consumers appreciate or avoid elements that prevent consumers from accepting information collection. We study how consumers trade off five privacy elements relating to distributive fairness (i.e., information collection, storage, use) and procedural fairness (i.e., transparency, control). Moreover, we analyze to what extent the impact of these elements differs between four industries that vary in information sensitivity and interaction intensity. By using a choice-based conjoint experiment we show that differences in information collection and use matter more in highly sensitive industries, while storage matters less. The impact of interaction intensity on the privacy elements is less pronounced. However, in interaction-intensive industries transparency matters less and consumers are generally less inclined to accept information collection. We discuss the implications from our results and show how firms can optimize their strategies in order to promote privacy.



This paper is based on Beke, Frank T., Felix Eggers (2017), "Promoting Privacy: How Consumers Trade Off Privacy Elements", working paper

## 4.1 Introduction

Over the past decade, firms have become customer-centered and relationship-driven. As this demands firms understanding the needs and preferences of individual consumers, collecting personal information about individual consumers has become imperative (Rust and Huang 2014). Digitalization and the '*Internet of Things*' enable firms to connect with their customers, and gather valuable information about them. However, driven by controversial revelations about privacy in general, such as Edward Snowden's disclosures about information collection and surveillance programs, consumers have become worried about how firms handle their information and respect their privacy (TRUSTe 2016).

Privacy concerns threaten firms, as they might prevent consumers from accepting information collection, or from using products and services that are conditional on collecting information, such as loyalty or personalization programs, mobile apps, and '*smart*' devices. As an example, a recent study by Pew Research shows that 60% of consumers have chosen to not install a mobile app when the collection of information was too extensive, and 43% have uninstalled a mobile app after finding out about information collection (Olmstead and Atkinson 2015). Even when consumers might not immediately abandon firms that neglect privacy it could result in backlash when consumers find out about their privacy practices afterwards.

The increased attention on privacy could also be seen as an opportunity for firms (Goldfarb and Tucker 2013). If firms want to convince consumers to accept (data-driven) products and services, differentiating in terms of privacy practices might lead to a higher probability of consumers choosing the firm with a favorable privacy strategy. As discussed in chapter 1, we define (informational) privacy as "*the extent to which a consumer is aware of and has the ability to control the collection, storage, and use of personal information by a firm"*. Accordingly, and in line with prior research (e.g., Hong and Thong 2013), we suggest

that firms can optimize their privacy strategy along five main elements (privacy practices): information collection, information storage, information use, transparency with regard to these elements, and control over these elements. In order to differentiate and promote their privacy strategy firms need a better understanding how these privacy elements affect consumers' decisions (Bolton and Saxena-Iyer 2009; Rust and Huang 2014). Therefore, we aim to answer the following research question: *What is the (relative) influence of the main elements of a firm's privacy strategy (information collection, information storage, information use, transparency, control) on consumers' acceptance of information collection?* In line with this focus, we concentrate on situations in which firms actively promote their privacy strategy to convince consumers to accept information collection. As a secondary research focus, we look at differences in effects between industries (or sectors) that are characterized by high or low information sensitivity (referring to the potential loss for consumers when information ends up in the wrong hands) and high or low interaction intensity (referring to how often consumers interact or transact with a firm).

While the influence of each privacy element on the acceptance of information collection has been studied before, our main contribution is that we derive the (relative) influence of the main privacy practices when studied in combination. Prior studies have mostly compared the influence of (one element of) privacy to other, non-privacy related elements, such as monetary compensation (e.g., Hann et al. 2007; Krafft, Arden, and Verhoef 2017). Providing insights into the extent to which other, unrelated elements can compensate for a lack of privacy is relevant for optimizing the overall market offering but it offers firms no guidance with regard to optimizing and promoting their privacy strategy. Moreover, whereas previous research has studied privacy elements that are not under immediate managerial control, such as the type of information collected (e.g., Phelps, Nowak, and Ferrell 2000; Roeber et al. 2015), we contribute by focusing on elements that a firm can change.

Moreover, many prior studies have assessed information collection in general (Röber et al. 2015; Son and Kim 2008), which neglects that consumers' privacy preferences can be context-specific (Laufer and Wolfe 1977; Nissenbaum 2004; Stewart 2017). Therefore, we analyze to what extent the influence of privacy on consumers is moderated by industry characteristics that enhance the risks (information sensitivity) or augment the benefits (interaction intensity).

Using a choice-based conjoint (CBC) experiment with 841 consumers and simulations nested in the current status quo of the industry, we find that all privacy elements matter to consumers. Information collection and use are more important in information-sensitive industries, whereas information storage is less relevant in these industries. Comparing industries based on interaction intensity leads to less pronounced differences, except that consumers require more transparency in industries that they do not interact frequently with. Moreover, in interaction-intensive industries consumers are less inclined to accept a service contingent on information collection in general. Across all industries, providing and promoting transparency and control constitutes a promising differentiation strategy to be considered.

### 4.2 Conceptual background

Although the attention for privacy has grown (Rust and Huang 2014; Wedel and Kannan 2016), firms still suffer from a limited understanding how their privacy strategy affects consumers. In line with social contract theory (Donaldson and Dunfee 1994) consumers take both the outcomes (distributive fairness) and the procedures (procedural fairness) of privacy into account. More specifically, distributive fairness refers to consumers' privacy calculus, which has been conceptualized as consumers' context-specific trade-off of the positive and negative outcomes (or consequences) of the collection, storage, and use of information (Dinev and Hart 2006; Laufer and Wolfe 1977). Consumers also care about how these outcomes are

created. In the context of privacy, procedural fairness revolves around transparency and control, which implies that firms need to convince consumers they are open and honest about their privacy practices and provide consumers a say over these privacy practices (Culnan and Armstrong 1999; Culnan and Bies 2003; Son and Kim 2008). Before discussing each privacy element in detail, Table 4-1 exhibits the main elements of a firm's privacy strategy, what they entail from the viewpoint of the firm, and where we focus on with regard to these elements.

**Table 4-1**. Definitions of main constructs

| **Construct** | **Our definition** | **Our focus** |
|---|---|---|
| Information Collection | Gathering and recording information about consumers | How and where? |
| Information Storage | Saving information and keeping it available for (future) use | How and how long? |
| Information Use | Examining information and employing the knowledge internally or externally | How and what for? |
| Transparency | Informing consumers about the collection, storage, and use of information | About what? |
| Control | Providing consumers the ability to determine who collects, stores, and uses which information for which purposes | Over what? |

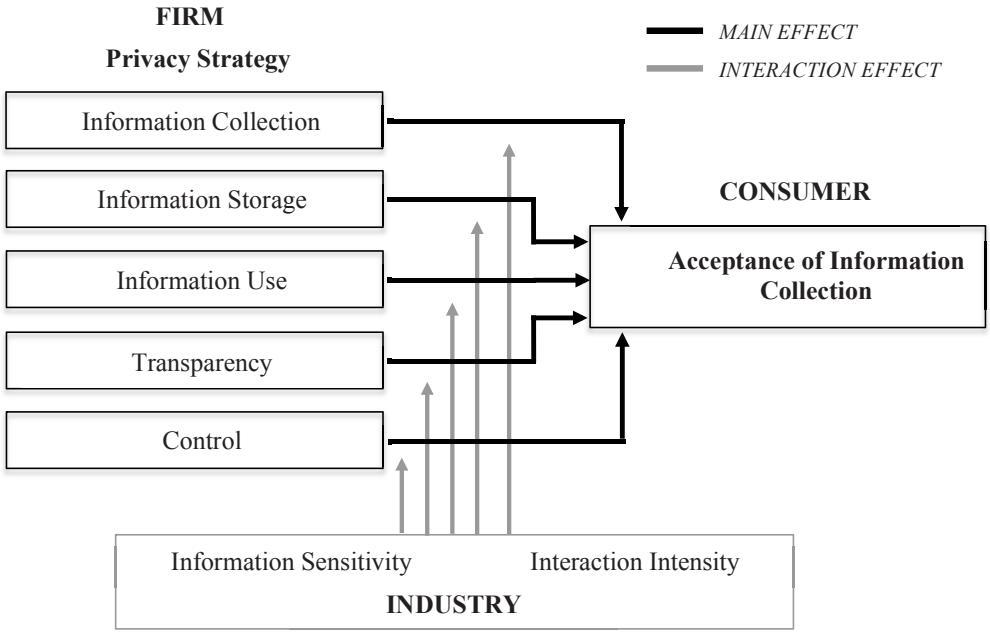



**Figure 4-1**. Conceptual model

Figure 4-1 summarizes the theory and conceptual model of our study. We study the effect of the main elements of a firm's privacy strategy on the acceptance of information collection and analyze the moderating effect of industry characteristics. We assess one industry characteristic that could aggravate the risks (information sensitivity) for consumers, and another industry characteristic that could enhance the benefits (interaction intensity) for consumers.

### *4.2.1 Information collection*

Information collection refers to a firm gathering and recording information about consumers. Prior work has shown that consumers are affected by the amount and type(s) of information a firm collects (Hui, Teo, and Lee 2007; Martin, Borah, and Palmatier 2017). When a firm collects more or more sensitive information the (potential) negative consequences consumers endure increase as well (Mothersbaugh et al. 2012). However, the type of information (and

therefore information sensitivity) is often industry- or sector-specific and therefore difficult to change for a firm. Instead, firms have to make a strategic decision about '*where*' and '*how'* – actively provided by consumers, passively tracked by firms or inferred from other information (World Economic Forum 2014b) – they collect information.

Digitalization enables firms to augment actively provided (volunteered) information with passively collected information about actual usage behavior, both internally, via their own channels (e.g., own website), and externally, via other channels (e.g., other websites, social media). Whereas consumers are generally permissive when a firm monitors their behavior via their own channels, they are more reluctant to provide access to externally collected information (Heimbach, Gottschlich, and Hinz 2015). Besides that consumers might consider such information collection more sensitive (and thus more risky) their reluctance can be explained by a lack of congruency between the products or services a firm offers and the externally collected information. Consumers might consider it abnormal that a firm wants to collect external information (Nissenbaum 2004, 2011) and fail to understand why external information collection would benefit them.

In addition to actively provided (volunteered) and passively tracked information, firms also make inferences about consumers based on collected information. For example, firms infer consumers' preferences based on their search behavior (Acquisti, Brandimarte, and Loewenstein 2015). While consumers could benefit from a firm's improved understanding of their needs and preferences, consumers consider drawing (harmful) inferences as undesirable (Culnan 1993). Specifically, consumers might still be hesitant towards inferred information as the inferences might not be transparent and even inaccurate, leading to negative consequences. The influence of the extent a firm infers information on consumers' acceptance of information collection is yet to be studied in more detail.

### *4.2.2 Information storage*

Once the information is collected, information storage implies that firms save the information in their database and keep it available for (future) use. When a firm fails in storing information safely – such as when information is stolen or accidently leaked – consumers respond negatively (Martin, Borah, and Palmatier 2017). The opposite is also true so that consumers respond positively when a firm promises safe storage. For example, consumers are more inclined to choose firms when only authorized personnel has access to information about customers (Hann et al. 2007), and use a personalized mobile app more often when information about them is stored only locally (Sutanto et al. 2013). However, there is a research gap in specific measures to improve information storage and whether these improvements are influential in convincing consumers to accept information collection.

In line with risk theory (Peter and Tarpey 1975), which suggests that consumers determine risks based on the probability and severity of a consequence, firms have two options for lowering the risk of information storage failures. First, a firm can try and reduce the probability that information storage failures occur, which is what both examples mentioned above aim to achieve (Hann et al. 2007; Sutanto et al. 2013). Firms can also reduce the chance of a storage failure by altering how long information is stored. When information is ephemeral it is less likely that the information ends up in the wrong hands. However, reducing storage time also limits a firm's ability to use the information. Therefore, a firm has to decide whether the usage constraint of shortening the storage time is offset by the positive effect on consumers' acceptance of information collection.

The other option to reduce the risk of information storage failures is to reduce the impact of such failures. Consumers suffer less negative consequences when anonymous information is stolen or accidently leaked than when identifiable information is lost (Jiang, Heng, and Choi 2013). Firms could therefore choose to store information in anonymous form,

i.e., without identifier, or whether it remains identifiable, for example based on name or email address. While storing information without identifier might reduce the risks for consumers, firms need to consider whether this compensates for the restricted possibilities of using the information.

### *4.2.3 Information use*

Once collected and stored, firms aim to use information in ways that create value for them and also for their customers (Verhoef, Kooge, and Walk 2016). Information use entails that firms examine the information they have collected and stored to generate knowledge about their customers. To create value, firms then employ this knowledge internally, to improve their products or services, or externally, by sharing the knowledge with third parties.

Increasingly, firms tailor their services or content to the needs and preferences of individual consumers (Adomavicius and Tuzhilin 2005; Montgomery and Smith 2009). Although consumers generally respond positively to personalized websites (Hauser et al. 2009; Hauser, Liberali, and Urban 2014; Mothersbaugh et al. 2012) and marketing content, such as advertisements and direct mail (Urban et al. 2013), personalization can also arouse privacy concern or reactance (Aguirre et al. 2015; Bleier and Eisenbeiss 2015a; b; Goldfarb and Tucker 2011b). When explicitly asked consumers have opposed personalized marketing content, such as banner ads or direct mail (Turow et al. 2009). Justifying personalized marketing content by pointing to increased relevance only convinced consumers to accept information collection in specific circumstances (Schumann, Von Wangenheim, and Groene 2014). Therefore, as consumers seemingly underestimate the added value of personalized marketing content when made explicit, it remains unclear whether it prompts consumers to accept information collection.

Besides personalizing marketing content, the knowledge about consumers also enables firms to provide consumers with personalized insights or recommendations, as firms have a

thorough understanding of how consumers behave and what they like. These personalized services are (more) relevant (Mothersbaugh et al. 2012; Wirtz and Lwin 2009), and thus consumers make more and longer use of services that provide such personalized recommendations (Chung, Rust, and Wedel 2009; Chung, Wedel, and Rust 2016). However, it remains to be seen whether promising personalized insights or recommendations motivates consumers to accept information collection, and whether consumers consider these practices more attractive than personalized marketing content.

Besides using information within the firm, disseminating the knowledge to external third parties might also generate additional revenue or provide more relevant advertising due to profiling (Awad and Krishnan 2006). There are no clear immediate benefits for consumers of such actions but they rather increase the risks, considering that consumers lose sight and control over their information. Therefore, consumers generally oppose '*secondary disclosure'* (Alreck and Settle 2007; Wirtz and Lwin 2009). What remains to be seen, however, is how severe the effect of secondary disclosure is on the acceptance of information collection.

#### *4.2.4 Transparency*

Another element of a firm's privacy strategy is transparency, which can be defined as informing consumers about the collection, storage, and use of personal information. Given that without transparency consumers cannot know whether their privacy is respected or violated, transparency is fundamental for privacy. The Federal Trade Committee (FTC) in the US has traditionally stressed the importance of transparency (Ohlhausen 2014), while transparency also serves as a crucial element for the General Data Protection Regulation (GDPR) that will be implemented in 2018 in the EU.

Even though governments enforce transparency, firms have remained reluctant to clearly inform consumers. Rather than motivating consumers to read privacy statements most firms conform to privacy legislation by posting long and difficult-to-read privacy statements

(McDonald and Cranor 2008). What remains unclear is whether being proactive and clearer about the collection, storage, and use of information could also benefit firms. Prior research has shown that perceived transparency makes consumers more cooperative and committed to a firm in general (Son and Kim 2008), and that actual transparency makes consumers feel less vulnerable (Aguirre et al. 2015; Martin, Borah, and Palmatier 2017). Thus, a firm could potentially benefit from being considered fair by being pro-actively transparent about the collection, storage, and use of information.

However, firms need to take into account that transparency might also raise awareness or arouse privacy concerns (LaRose and Rifon 2007). Over 70% of consumers is unaware which information firms collect, and those consumers that are aware are less willing to disclose information (Rose, Rehse, and Röber 2012), which implies that transparency could be a double-edged sword. Therefore, understanding whether promoting transparency about the collection, storage, or use of information truly affects consumers positively is crucial.

#### *4.2.5 Control*

Control implies that a consumer has the ability to determine who collects, stores, and uses which information for which purposes. As discussed in chapter one, privacy is contingent on control. The importance of control is also reflected in the opinion of the FTC on privacy, which has stressed firms should ask consumers for consent (Ohlhausen 2014). Meanwhile in the EU, the upcoming GDPR mandates that besides control over information collection (*consent of collection*), firms should also provide consumers with control over information storage (*ability to remove data*) and information use (*ability to prevent the use of data,* General Data Protection Regulation 2018). Thus, legislation considers privacy to be violated when information is collected, stored, and used against the will of consumers.

Besides being enforced by governments, providing control might also be in the interest of firms. The majority of consumers want control over their information (PWC 2014), and

prior research has shown that consumers are more cooperative and committed to firms they believe provide control (Son and Kim 2008). Several studies have focused on control over either information collection, or information storage, or information use. For example, providing control over the collection of information increases the effectiveness of personalized advertisements (Schumann, Von Wangenheim, and Groene 2014). Providing consumers control over storage by offering the opportunity to remove information increases their acceptance of information collection by firms in general (Röber et al. 2015). Moreover, control over the use of information makes consumers feel less vulnerable (Martin, Borah, and Palmatier 2017) and more willing to self-disclose information to a specific firm (Mothersbaugh et al. 2012).

However, despite governmental pressure and the (potential) benefit for both firms and consumers, firms have remained reluctant to pro-actively communicate that consumers have influence over the collection, storage, and use of information. Anecdotal evidence seems to suggest that firms are anxious that providing control allows consumers to disrupt the collection, storage, and use of information. Therefore, they need to consider carefully whether offering control truly affects the acceptance of information collection. Moreover, firms need a better understanding whether consumers' acceptance of information collection hinges more on having the ability to prevent information collection (control over collection), the ability to remove or alter information (control over storage), or the ability to determine how information is used (control over use).

#### *4.2.6 Industries: Information sensitivity and interaction intensity*

Given that consumers' privacy preferences are context-specific (Martin and Nissenbaum 2016a; Nissenbaum 2004) the influence of managerial decisions with regard to privacy could also be altered by the industry a firm operates in. As depicted in Table 4-2, we will assess the influence of one industry characteristic that could enhance the (perceived) risks for consumers

(information sensitivity), and another industry characteristic that could affect the (perceived) benefits for consumers (interaction intensity).

*Information sensitivity*

Information sensitivity reflects the potential loss (‘*risk*’) consumers might suffer when the information ends up in the wrong hands and is misused (Milne et al. 2017; Mothersbaugh et al. 2012). Consumers generally consider financial or medical information as more sensitive than lifestyle or purchase habits (Mothersbaugh et al. 2012). While consumers have shown to be less willing to disclose sensitive information (Acquisti, John, and Loewenstein 2012; Lwin, Wirtz, and Williams 2007; Mothersbaugh et al. 2012; Phelps, Nowak, and Ferrell 2000; Röber et al. 2015), these studies have manipulated information sensitivity by asking respondents to disclose a wide variety of types of information. However, firms have generally limited influence on which information is available for them to collect. For example, a bank needs to process payment information in order to provide personalized services, even though consumers might consider that information very sensitive. Given that information sensitivity is under limited managerial control, firms need a better understanding of the moderating role of information sensitivity on their privacy strategy.

Bart and colleagues (2005) showed that privacy has a more profound influence on the value of websites when the information risk, which they define along the same lines as information sensitivity, of a website is high. What they do not assess however is whether the increased risk alters the influence of (one of) the privacy elements. We expect that in industries in which the risk is higher, as is the case when sensitive information is collected, consumers are especially more reactive to where and how the information is collected. In situations in which the (potential) negative consequences (risks) are very severe consumers generally aim to avoid these risks (Dowling 1986). While in this context the storage and (to a lesser extent) use of information could diminish the risks for consumers, the only way to

**Table 4-2**. Definitions of moderators

| Construct | Definition |
|---|---|
| Information Sensitivity | The potential loss consumers might suffer when information ends up in the wrong hands |
| Interaction Intensity | The frequency with which consumers interact or transact with a firm |

entirely avoid these intensified risks is by not allowing firms to collect information, i.e., not allowing firms to collect information internally, externally or by inferring information. Therefore, as we expect that in information sensitive industries consumers will be more focused on information collection we hypothesize the following:

> $H_{1a}$: The relative importance of information collection is higher when information sensitivity of an industry is high

Besides avoiding the risks altogether, consumers can also take on a more active approach in managing the risks (Dowling 1986), which implies monitoring the risks (transparency) and intervening (control) when necessary. Prior research has also shown that providing transparency is more effective in decreasing feelings of violation when consumers believe they are more susceptible to harm due to unwanted uses of their personal information (Martin, Borah, and Palmatier 2017). Similarly, the effect of (perceived) control on information disclosure is larger for sensitive information than for less sensitive information (Mothersbaugh et al. 2012). These findings seem to suggest that transparency and control (procedural fairness) matter more when consumers believe they are more at risk, as they aim to manage these risks more meticulously. Therefore, we hypothesize the following:

> $H_{1b}$: The relative importance of transparency is higher when information sensitivity of an industry is high

$H_{1c}$: The relative importance of control is higher when information sensitivity of an industry is high

Note that our hypotheses relate to the (relative) importance of privacy elements. Therefore, considering that we hypothesize an increased importance of information collection, transparency and control this implies that information storage and use are (relatively) less important in information-sensitive industries.

*Interaction intensity*

Besides having an influence on the risks for consumers, the type of industry might also affect the benefits consumers derive from the collection, storage, and use of information. We propose that the benefits are affected by the intensity a consumer interacts with a firm. Interaction intensity, which we define as the frequency with which consumers interact or transact with a firm, has been used to classify industries or firms by many prior studies using many comparable terms: usage level (Danaher, Conroy, and McColl-Kennedy 2008), high vs. low contact (Bowen 1990), and visit frequency (Hann et al. 2007). The value consumers derive from improved service is enhanced in industries in which consumers interact frequently with a firm from that specific industry. For example, consumers benefit more from a more efficient checkout process when they transact more often with that firm. Similarly, consumers consider personalized feedback or marketing content more valuable when they use the products and services more often (Mothersbaugh et al. 2012), while Ashley and colleagues (2011) show that consumers are more open to relationship programs with firms they interact frequently with.

However, prior research does not yet address to what extent the interaction frequency affects the influence of specific elements of a firm's privacy strategy. In line with regulatory focus theory (Higgins 1997), we believe that in industries with a high interaction frequency the (potential) benefits are more profound, shifting consumers' focus to those elements that

(might) provide a benefit as well. In this context the use of information drives the benefits firms provide to consumers, as it enables firms to increase the relevance of their content (e.g., direct mail), saving consumers time and providing valuable information. Therefore, we suggest that in industries with high interaction intensity consumers are more focused on benefits —derived from the use of information—and thus hypothesize the following:

> $H_{2a}$: The relative importance of information use is higher when interaction intensity of an industry is high.

Even when consumers are focused on obtaining benefits, they might still want to diminish the risks without giving up these benefits. Preventing the collection of information or restricting how (long) information is stored hinders firms in providing valuable products and services, which makes information collection and storage less relevant. The only way for consumers to diminish the risks while preserving the (potential) benefits is by actively managing their privacy (Dowling 1986), which, as discussed above, would make transparency and control relatively more important. Thus, while consumers would allow firms to collect and store information in order to maximize the (potential) benefits of personalization, they would monitor and prevent undesirable privacy strategies at the same time. Therefore, relative to the other privacy elements, we hypothesize the following:

> $H_{2b}$: The relative importance of transparency is higher when interaction intensity of an industry is high.

> $H_{2c}$: The relative importance of control is higher when interaction intensity of an industry is high.

As for information sensitivity, the hypotheses relate to the (relative) importance of privacy elements. Therefore, considering that we hypothesize an increased importance of information

use, transparency, and control, this implies that information collection and information storage are (relatively) less important in interaction-intensive industries.

## 4.3 Research design

### *4.3.1 Experimental design and procedure*

In order to measure the moderating role of industry characteristics on the influence of a firm's privacy strategy, we employed a 2 x 2 between-subjects design, varying in information sensitivity (high vs. low) and interaction intensity (high vs. low) of the industry. We selected specific industries based on a pre-test (N = 50), in which respondents had to rate 16 industries on information sensitivity and interaction intensity, among other characteristics. All characteristics were rated on 7-point Likert scale, using bipolar anchors (e.g., insensitive (1) … sensitive (7) for information sensitivity, see Appendix E for an overview of the industry classification). As depicted in Figure 4-2, we identified banks, (healthcare) insurances, news (providers), and cinemas as the four industries covering the four experimental conditions.

In our main study respondents were allocated randomly to one of the four conditions, and had to indicate with which firm they normally transacted within the industry allocated. All questions were adjusted to that specific firm thereafter so that we assess the acceptance of information collection for a specific purpose by a specific firm within a specific industry (see Appendix F for the scenario). Respondents were screened out if they did not interact with a firm from the industry, as these respondents would not be able to relate the subsequent conjoint experiment to a specific, realistic context.

Before the conjoint section started the respondents had to answer several questions about the privacy strategy of their current firm. These questions were structured into the privacy elements information collection, information storage, information use, transparency, and control. Besides providing a benchmark, we used the same terminologies as in the CBC experiment so that respondents could get familiar with the attributes and levels that were

| | | Interaction Intensity: High | Interaction Intensity: Low |
|---|---|---|---|
| **Information Sensitivity** | **High** | *Bank* | *Insurance (healthcare)* |
| | **Low** | *News (provider)* | *Cinema* |

**Figure 4-2**. Industry classification

used in the subsequent choice tasks. At the end of the survey, we measured the perceived information sensitivity and interaction intensity, consumers' commitment to the firm (behavioral loyalty, satisfaction, trust), consumers' general privacy concern and privacy protective actions, and some demographics (see Appendix D for an overview of all the measurement items).

### *4.3.2 Conjoint design*

In the CBC experiment, we assess whether consumers accept a personalization program that varies in the way information is collected, stored, and used, and the amount of transparency and control over these elements provided by a firm (see Appendix F for the scenario). For each of these elements we generated levels based on realistic combinations of subdimensions of each element, which resulted in seven to nine levels per element[7]. Specifically, for information collection we used seven combinations of whether the information was provided voluntarily, tracked within the channels of the firm (internally), tracked outside the channels of the firm (externally), and/or whether the information was inferred. Storage was represented by nine combinations of two subdimensions one that captured storage time (unlimited, one year, or one month) and another that captured storage type (anonymized, identifiable by ID, or identifiable by email address). Information use consisted of eight combinations of

[7] We made sure that each of the elements matter in a pretest using banks as the research context (N = 100).

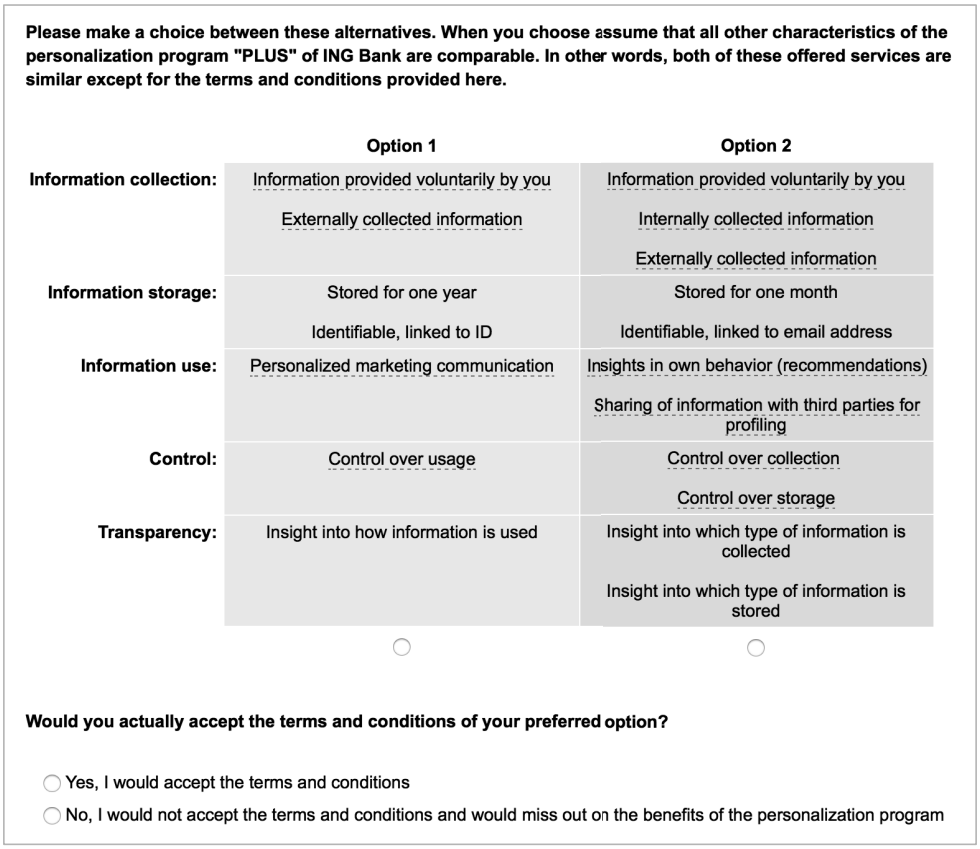
personalization of insights, personalization of marketing content, and secondary disclosure. Finally, transparency and control both featured all eight combinations for which element (collection, storage, use) the firm provides transparency and control (see Appendix G for the complete list of attributes and levels). Respondents were able to get more information about the meaning of the attribute levels by moving their pointer over each of the levels text throughout the experiment, which then opened a popup box with additional information and examples.

We used a computer-generated design in order to allocate randomized sets of profiles to choice sets with two options each. The resulting factorial design was balanced and orthogonal (Huber and Zwerina 1996). Moreover, as we are interested in whether consumers accept information collection or would rather reject information collection and not use the service, we also include a no-choice option using a dual-response format (Brazell et al. 2006; Wlömert and Eggers 2016). Figure 4-3 depicts an exemplary choice set. Each respondent completed 14 choice sets, including an initial training set and a holdout set for checking predictive validity so that twelve decisions remained for the estimation.

## 4.4 Results

### *4.4.1 Sample*

We invited respondents via a Dutch research panel to our experiment. Respondents received standard panel incentives for their participation. The median time to complete the survey was about 13 minutes (790 seconds). From the 1285 consumers who completed the survey, 100 respondents were discarded because they answered the survey in an unrealistically short time (less than 5 minutes), while another 344 respondents were removed due to failing an attention check. The remaining sample of 841 consumers showed no signs of adverse quality (e.g., straightlining) and was representative for the Dutch population. Respondents were equally divided over the four industries: Bank (N = 211), Insurance (N = 223), News (N = 202), and



**Please make a choice between these alternatives. When you choose assume that all other characteristics of the personalization program "PLUS" of ING Bank are comparable. In other words, both of these offered services are similar except for the terms and conditions provided here.**

| | Option 1 | Option 2 |
|---|---|---|
| **Information collection:** | Information provided voluntarily by you<br>Externally collected information | Information provided voluntarily by you<br>Internally collected information<br>Externally collected information |
| **Information storage:** | Stored for one year<br>Identifiable, linked to ID | Stored for one month<br>Identifiable, linked to email address |
| **Information use:** | Personalized marketing communication | Insights in own behavior (recommendations)<br>Sharing of information with third parties for profiling |
| **Control:** | Control over usage | Control over collection<br>Control over storage |
| **Transparency:** | Insight into how information is used | Insight into which type of information is collected<br>Insight into which type of information is stored |

**Would you actually accept the terms and conditions of your preferred option?**

- Yes, I would accept the terms and conditions
- No, I would not accept the terms and conditions and would miss out on the benefits of the personalization program

**Figure 4-3.** Exemplary choice set (bank setting, translated)

Cinema (N = 205). Table 4-3 shows a manipulation check based on perceived industry characteristics and confirms that the four industries were appropriately classified.

As target groups in the four industries differ there were minor structural differences between the samples. Specifically, the cinema sample was slightly younger and contained relatively more married people compared to the other industries. We checked and found no significant effects of age and marital status, or other demographic variables, on the results.

### *4.4.2 Status quo*

Table 4-4 shows that the (perceived) status quo of current privacy strategies differs between industries. According to the respondents' classification, news providers mainly seem to rely

**Table 4-3.** Manipulation check

| | Bank | Insurance | News | Cinema |
|---|---|---|---|---|
| **Interaction frequency** | High – 4.95 | Low – 2.69 | High – 4.09 | Low – 1.96 |
| **Information sensitivity** | High – 4.13 | High – 3.52 | Low – 3.03 | Low – 2.41 |

on externally collected or inferred information, while banks and insurers mainly depend on volunteered and (to a lesser extent) internally collected information. Information is largely stored for an unlimited time. Moreover, all industries are perceived to store identifiable information, either by ID (bank and news) or by email address (cinema and insurance). In terms of information use, banks and insurances rely mostly on providing insights in own behavior and recommendations, while news providers and cinemas are more focused on providing personalized marketing content. Over 40% of the respondents believed their news provider disseminates information to third parties. Finally, what stands out is that across all industries most respondents believe their firm is not transparent (avg. 67%) and provides no control (avg. 58.7%).

### *4.4.3 Estimation*

We estimated consumers' preferences for the privacy elements using a standard multinomial logit (MNL) model within a hierarchical Bayes (HB) procedure. By using a HB procedure we account for heterogeneity between consumers as it provides us with individual-level utility estimates. Accordingly, at the lower level, the probability that respondent $h$ chooses alternative $i$ from choice set $J$ can be written as (Rossi and Allenby 2003):

$$(1) \qquad \mathrm{P}(i)_h = \frac{\exp(\beta_h{}' x_i)}{\sum_{j \in J} \exp(\beta_h{}' x_j)},$$

with $x_i$ being a vector of attribute levels for alternative $i$ and $\beta_h$ being a vector of the partworth

**Table 4-4.** Current privacy strategy per industry (across respondents)

| Current privacy strategy | | Bank | Insurance | News | Cinema |
|---|---|---|---|---|---|
| **Collection** | | | | | |
| | Volunteered information | 87.68% | 91.48% | 56.93% | 80.98% |
| | Internally collected information | 71.56% | 60.09% | 64.36% | 65.37% |
| | Externally collected information | 24.65% | 20.63% | 42.08% | 28.29% |
| | Inferred information | 33.18% | 26.01% | 45.55% | 36.10% |
| | None of the above | 1.90% | 2.69% | 9.90% | 6.34% |
| **Storage (Time)** | | | | | |
| | One month | 4.27% | 1.79% | 11.81% | 5.85% |
| | One year | 23.22% | 21.53% | 24.75% | 34.63% |
| | Unlimited | 68.25% | 71.75% | 53.96% | 53.66% |
| | None of the above | 4.27% | 4.93% | 9.40% | 5.85% |
| **Storage (Type)** | | | | | |
| | Anonymous | 22.75% | 26.00% | 12.38% | 16.59% |
| | Identifiable on ID | 53.56% | 27.35% | 66.34% | 12.68% |
| | Identifiable on email address | 21.80% | 41.70% | 19.80% | 67.32% |
| | None of the above | 1.90% | 4.93% | 1.49% | 3.42% |
| **Information Use** | | | | | |
| | Insights in own behavior | 72.99% | 60.54% | 41.09% | 55.61% |
| | Personalized marketing content | 58.77% | 52.92% | 70.30% | 75.61% |
| | Dissemination with third parties | 13.27% | 16.59% | 40.10% | 26.83% |
| | None of the above | 9.95% | 17.04% | 12.87% | 13.27% |
| **Transparency** | | | | | |
| | Insight in collection | 19.90% | 20.62% | 20.79% | 16.59% |
| | Insight in storage | 16.11% | 16.59% | 11.88% | 13.17% |
| | Insight in use | 13.74% | 12.11% | 16.34% | 15.61% |
| | None of the above | 67.23% | 65.02% | 66.34% | 69.76% |
| **Control** | | | | | |
| | Control over collection | 21.33% | 24.66% | 26.24% | 29.27% |
| | Control over storage | 16.11% | 10.31% | 14.36% | 15.11% |
| | Control over use | 23.22% | 16.59% | 19.80% | 23.90% |
| | None of the above | 59.24% | 63.68% | 58.42% | 53.17% |

utilities for respondent $h$. At the upper level, we assume a normal distribution of the partworths with different means according to the two industry characteristics:

(2) $$\beta_h = \theta' z_h + \varepsilon_h,$$

with $\theta$ being a matrix of parameters, $z_h$ being a vector of covariates (information sensitivity, interaction intensity), and $\varepsilon_h$ representing normally distributed random effects with covariance matrix $D$, i.e., $\varepsilon_h \sim Normal(0, D)$.

We used the RSGHB package in R to estimate the model, which is based on the MCMC algorithm with a Gibbs sampler. After a burn-in period of 10,000 iterations we used 10,000 iterations to draw posterior partworths.

The model fit was acceptable with 45.9% of uncertainty explained in the estimation sample ($U^2$, Hauser 1978). The holdout sample predictions among three alternatives (two privacy alternatives and no-choice) outperformed a chance model 2:1 (hit rate = 0.712). We found no substantial improvement in model fit when considering interaction effects so that we only report main effects.

#### *4.4.4 Estimation results*

Table 4-5 provides the mean and standard deviations of the posterior means. We present the results as contrasts between the two industry characteristics. Overall, the coefficients show face validity.

Collecting more information than voluntarily provided has a negative effect, and provides more disutility in information sensitive and interaction intensive industries. The effect of internal information collection is, however, close to zero. The standard deviations indicate that in all industries a proportion of the consumers consider internal information collection and (to a lesser extent) inferring information as beneficial. In contrast, collecting information externally has a substantial negative effect on the acceptance of the

**Table 4-5.** Estimation results contrasts

| | Information sensitivity | | | | Interaction intensity | | | |
|---|---|---|---|---|---|---|---|---|
| | Low | | High | | Low | | High | |
| | **Mean** | **SD** | **Mean** | **SD** | **Mean** | **SD** | **Mean** | **SD** |
| **Collection** | | | | | | | | |
| *Voluntary* | (0.00) | | (0.00) | | (0.00) | | (0.00) | |
| Internal | -0.02 | 0.20 | -0.06 | 0.20 | 0.01 | 0.20 | -0.10 | 0.20 |
| External | -0.33 | 0.28 | -0.51 | 0.27 | -0.44 | 0.28 | -0.39 | 0.29 |
| Inferred | -0.19 | 0.27 | -0.22 | 0.27 | -0.17 | 0.27 | -0.24 | 0.27 |
| **Storage (Time)** | | | | | | | | |
| *Unlimited* | (0.00) | | (0.00) | | (0.00) | | (0.00) | |
| One year | 0.48 | 0.32 | 0.39 | 0.32 | 0.46 | 0.32 | 0.41 | 0.32 |
| One month | 0.79 | 0.51 | 0.48 | 0.51 | 0.58 | 0.52 | 0.69 | 0.54 |
| **Storage (Type)** | | | | | | | | |
| *Anonymous* | (0.00) | | (0.00) | | (0.00) | | (0.00) | |
| ID number | -1.82 | 1.09 | -0.97 | 1.04 | -1.39 | 1.10 | -1.36 | 1.20 |
| Email address | -1.30 | 0.88 | -1.05 | 0.79 | -1.10 | 0.80 | -1.24 | 0.88 |
| **Use** | | | | | | | | |
| *None* | (0.00) | | (0.00) | | (0.00) | | (0.00) | |
| Personalized insights | -0.02 | 0.12 | 0.03 | 0.12 | 0.00 | 0.13 | 0.01 | 0.12 |
| Marketing content | -0.17 | 0.15 | -0.17 | 0.15 | -0.20 | 0.15 | -0.14 | 0.15 |
| Dissemination | -0.85 | 0.78 | -1.00 | 0.81 | -0.96 | 0.81 | -0.89 | 0.79 |
| **Transparency** | | | | | | | | |
| *None* | (0.00) | | (0.00) | | (0.00) | | (0.00) | |
| Collection | 0.21 | 0.23 | 0.22 | 0.23 | 0.27 | 0.22 | 0.16 | 0.23 |
| Storage | 0.19 | 0.15 | 0.19 | 0.15 | 0.20 | 0.15 | 0.18 | 0.15 |
| Use | 0.19 | 0.24 | 0.26 | 0.23 | 0.30 | 0.23 | 0.15 | 0.22 |
| **Control** | | | | | | | | |
| *None* | (0.00) | | (0.00) | | (0.00) | | (0.00) | |
| Collection | 0.28 | 0.14 | 0.31 | 0.16 | 0.28 | 0.15 | 0.32 | 0.15 |
| Storage | 0.26 | 0.18 | 0.21 | 0.18 | 0.26 | 0.18 | 0.21 | 0.18 |
| Use | 0.38 | 0.27 | 0.46 | 0.27 | 0.42 | 0.26 | 0.42 | 0.28 |
| **No Choice** | -0.73 | 2.59 | -0.56 | 2.74 | -0.88 | 2.59 | -0.39 | 2.72 |

*Reference category in italics*
*Mean = mean across respondents, SD = standard deviation across respondents*
*NOTE: Some attributes consist of levels based on combinations,*

personalization program. The absolute magnitude of the mean effect exceeds the standard deviation in all industries, in particular in information sensitive industries.

On average, consumers react in a neutral way regarding the use of information for personalization of insights and recommendations. Again, the standard deviations indicate that across all industries some consumers perceive a utility of this use while others a disutility. Personalized marketing content has a negative influence although there are some consumers who are indifferent or even perceive a benefit. Respondents are consistently averse towards disseminating information to third parties (e.g., other firms), in particular in industries that are characterized by a high information sensitivity and low interaction intensity.

On average, consumers respond in a positive manner to transparency and control, although effect sizes are smaller for transparency. Standard deviations often exceed the means such that some consumers consider transparency as negative in industries with low information sensitivity and with which they frequently interact. Overall, transparency is most preferred in industries with which consumers interact less frequently. Among the three elements (collection, storage, and use of information), transparency and control have, on average, the smallest effect sizes for storage, i.e., consumers are more sensitive towards transparency and control over collection and use of information. These effects are more pronounced for control than for transparency and in information sensitive and interaction intensive industries. Nevertheless, across all industries it is most beneficial from a consumer perspective to provide control over all elements, while no control is the worst strategy.

Finally, the mean coefficient for the no-choice option is negative, indicating that consumers are more likely choose a privacy strategy at the reference categories than not to accept the information collection. In particular, in interaction intensive industries consumers are more inclined to opt for the no-choice option and not accept the personalization program (i.e., the mean effect size is less negative). The magnitude of the none parameter suggests that

consumers are less likely to accept information collection (i.e., the none threshold is undercut by the parameter of respective privacy elements), for example, if information is stored in an identifiable way or if information is shared with third parties. This, however, can be compensated for by other positive elements. Within industries there is considerable heterogeneity in consumers' preferences, i.e., some respondents are very hesitant to accept a service contingent on information collection while others react less sensitive.

*Relative importance*

The previous chapter illustrates that there are differences in consumers' preferences based on information sensitivity and interaction intensity. Based on the difference between best and worst strategies per element, Table 4-6 shows the mean relative importance rates depending on the industry characteristics (calculated for each individual in each draw, then averaged). While storage type matters most in almost all industries, storage time is less important. Storage type and time are less important for information sensitive industries, while information collection and use gain in importance weight. Differences in transparency and control depending on information sensitivity are only marginally significant.

Regarding interaction intensity, importance weights are more balanced. We only see significant differences in terms of transparency, which is more relevant in industries that are characterized by less frequent interactions (here: insurances and cinemas). We will discuss whether our hypotheses are confirmed or rejected in the discussion section below.

### *4.4.5 Simulation and sensitivity analysis*

The previous analyses focus on the effect of privacy elements on consumers' preferences, i.e., utility estimates. However, they do not yet consider if the differences in utilities are meaningful in terms of their effect on choice probabilities. To analyze these effects we create a scenario in which we predict the share of consumers that would adopt the personalization

**Table 4-6.** Moderating effect of industry characteristics on relative importance rates

| | Information sensitivity | | | | Interaction intensity | | | |
|---|---|---|---|---|---|---|---|---|
| | **Low** | **High** | **Difference** | **p** | **Low** | **High** | **Difference** | **p** |
| **Collection** | 0.141 | 0.160 | 14% | 0.003 | 0.150 | 0.152 | 1% | 0.381 |
| **Storage** (Time) | 0.123 | 0.111 | -10% | 0.018 | 0.114 | 0.120 | 5% | 0.131 |
| **Storage** (Type) | 0.250 | 0.205 | -18% | 0.000 | 0.224 | 0.230 | 3% | 0.180 |
| **Use** | 0.199 | 0.216 | 9% | 0.007 | 0.211 | 0.204 | -3% | 0.146 |
| **Transparency** | 0.136 | 0.145 | 6% | 0.082 | 0.146 | 0.135 | -7% | 0.036 |
| **Control** | 0.152 | 0.163 | 7% | 0.071 | 0.155 | 0.159 | 2% | 0.326 |

*NOTE: p-values are based on distribution of posterior draws*

program rather than not accept the information collection that goes along with it. Specifically, we use the logit model (Equation 1) to predict choice probabilities among two alternatives: (1) the current status quo within the industry and (2) the no-choice option. To determine the current status quo we consider all privacy elements that more than 33%[8] of the consumers indicated as currently being used by the firm within the industry.

According to Table 4-7, the status quo of privacy strategy has an average choice probability of less than 50% in all industries, i.e., on average it is more likely that consumers do not consent to the information collection. The highest probability of 0.45 is achieved by the insurance industry in which only internal information is collected, stored by email address for unlimited time, and used for personalized insights and marketing content. News providers obtain the lowest choice probability in comparison (0.27) because their strategy contains more negative elements, i.e., internal and external information collection, plus inferred information that are used for personalized insights and marketing content, and dissemination of information to third parties.

[8] We use one third because this value implies differences between industries while still considering only frequently employed strategies.

**Table 4-7.** Sensitivity analysis

| | Bank | | | Insurance | | | News | | | Cinema | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Status quo** | | 0.39 | | | 0.45 | | | 0.27 | | | 0.44 | |
| **Collection** | | | | | | | | | | | | |
| Internal | - | 0.01 | 2% | - | 0.00 | 1% | - | 0.00 | 0% | - | -0.01 | -1% |
| External | + | -0.05 | -12% | + | -0.05 | -10% | - | 0.02 | 6% | + | -0.04 | -9% |
| Inferred | - | 0.03 | 8% | + | -0.02 | -4% | - | 0.01 | 5% | - | 0.02 | 4% |
| **Storage (Time)** | | | | | | | | | | | | |
| Unlimited | 0 | 0.00 | 0% | 0 | 0 | 0% | 0 | 0 | 0% | 0 | 0 | 0% |
| One year | + | 0.03 | 8% | + | 0.04 | 8% | + | 0.03 | 12% | + | 0.06 | 12% |
| One month | + | 0.04 | 11% | + | 0.04 | 8% | + | 0.06 | 23% | + | 0.08 | 18% |
| **Storage (Type)** | | | | | | | | | | | | |
| *Anonymous* | + | 0.10 | 25% | + | 0.11 | 25% | + | 0.14 | 54% | + | 0.14 | 32% |
| ID number | 0 | 0.00 | 0% | + | 0.00 | 1% | 0 | 0 | 0% | + | -0.06 | -13% |
| Email address | + | -0.02 | -4% | 0 | 0 | 0% | + | 0.02 | 6% | 0 | 0 | 0% |
| **Use** | | | | | | | | | | | | |
| Insights | - | 0.00 | -1% | - | 0.00 | 0% | - | 0.00 | 1% | - | 0.00 | 1% |
| Content | - | 0.01 | 3% | - | 0.02 | 4% | - | 0.01 | 3% | - | 0.02 | 4% |
| Dissemination | + | -0.09 | -23% | + | -0.08 | -18% | - | 0.05 | 18% | + | -0.09 | -21% |
| **Transparency** | | | | | | | | | | | | |
| Collection | + | 0.02 | 4% | + | 0.02 | 5% | + | 0.01 | 5% | + | 0.03 | 7% |
| Storage | + | 0.02 | 5% | + | 0.02 | 4% | + | 0.01 | 4% | + | 0.02 | 5% |
| Use | + | 0.02 | 4% | + | 0.03 | 6% | + | 0.01 | 3% | + | 0.03 | 6% |
| All of the above | + | 0.05 | 14% | + | 0.07 | 14% | + | 0.03 | 12% | + | 0.08 | 18% |
| **Control** | | | | | | | | | | | | |
| Collection | + | 0.04 | 10% | + | 0.03 | 6% | + | 0.02 | 8% | + | 0.03 | 7% |
| Storage | + | 0.02 | 5% | + | 0.02 | 4% | + | 0.02 | 6% | + | 0.03 | 7% |
| Use | + | 0.05 | 12% | + | 0.04 | 9% | + | 0.03 | 11% | + | 0.04 | 10% |
| All of the above | + | 0.10 | 26% | + | 0.08 | 19% | + | 0.07 | 26% | + | 0.11 | 25% |

*NOTE: Privacy element added (+), removed (-), or status quo (0)*

Our sensitivity analysis compares to what extent the shares of the status quo scenario change when privacy elements are added (+) or removed (-) from the current strategy (0). The first column depicts the absolute change in choice probabilities and the second column the

relative change. Accordingly, firms should be reluctant to collect information externally, as the share of consumers accepting information collection would drop by 19% (cinema) to 12% (bank) when firms start collecting information externally. For news the influence of removing external information collection is less profound (6%), as consumers believe most news providers already collect information externally.

Storing information for a shorter period also seems to be a promising strategy, which would especially boost the acceptance of information collection by news providers (+23%) and cinemas (+18%). However, firms need to consider whether this positive effect offsets the usage constraint of shorting the storage time. The most influential lever to increase choice probabilities is to save personal information only in an anonymous form, e.g., at an aggregated level. In this case shares would increase by 25% (bank and insurance) to 54% (news). This strategy, however, would also limit the usage possibilities for a firm.

With regard to the use of information the largest negative impact has the dissemination of information to third parties, as 18% (insurance) to 23% (bank) of the current share would be lost when adding this element to the strategy. Also, news providers who are currently using this strategy would benefit largely from removing this element, resulting in +18% share increase. Removing other elements of information use only has a marginal effect, likely because they are already being used.

A firm could also maintain their current strategies instead, and add transparency and control elements. Each of these elements is able to increase choice probabilities. Adding all transparency and control elements would make the personalization program substantially more attractive so that the choice probabilities would exceed those of the no-choice option. This does not hold for news providers, however, given the low choice probability of the status quo. Overall, these results confirm that consumers are sensitive to optimizing the privacy strategy, i.e., that focusing on specific privacy elements matters.

## 4.5 Discussion

We study how the main elements of a firm's privacy strategy affect the acceptance of information collection. Moreover, we assess if the importance of each privacy element differs as hypothesized between industries that vary in information sensitivity and interaction intensity. The results of the hypothesis tests are depicted in Table 4-8. Overall, we see that each of the privacy elements (information collection, storage, use, transparency, and control) matter to consumers and that the effects differ systematically between industries.

More specifically, we observe that using more channels (methods) to collect information negatively affects the acceptance of information collection. This corresponds with prior work (e.g., Martin et al. 2017) that showed that consumers feel more vulnerable when a firm requests access to more (types of) information. Although interaction intensity increases the negative impact of internal information collection, this effect is negligible according to the sensitivity analysis. We find that in the status quo all industries already collect information internally. Hence, due to the status quo, removing this element only marginally affects the choice probabilities. Moreover, we show that consumers are more responsive towards information collection in industries that handle sensitive information, such as banks and insurance firms, thereby confirming our first hypothesis ($H_{1a}$). The risks are intensified in information sensitive industries, which suggests that consumers focus more on ways to avoid these risks altogether. The difference in the importance rate of information collection between sensitive and non-sensitive industries is mainly due to consumers opposing that firms from sensitive industries collect information via external sources. Consumers are more responsive when firms collect sensitive information that is incongruent with their products and services (Lwin, Wirtz, and Williams 2007; Nissenbaum 2004), which is more likely when external sources are involved. The sensitivity analysis also confirms that banks and insurance firms should be reluctant with collecting information from external

sources. Consumers want banks and insurance firms to focus on providing financial services rather than collecting seemingly irrelevant information, while news providers and cinemas collecting that same information seems easier to justify.

In line with risk theory, our findings show that promoting a shorter period for storing information and storing it anonymously increases consumers' acceptance of information collection. It is remarkable, however, that information storage is relatively less important in information sensitive industries (bank, insurance). Besides that these importance rates are relative and thus not necessarily imply that storage is less important on an absolute level, consumers might understand that banks and insurance firms need to store identifiable information for an extended period in order to provide reliable services. In industries in which information is less sensitive consumers might doubt the requirement to store identifiable information for an unlimited period. Furthermore, what is noteworthy is that in non-sensitive industries consumers seem to prefer that firms store information based on email address rather than ID number, while consumers are rather indifferent in other industries. However, the preference for storing by (the less anonymous) email address seems strongest in and thus primarily driven by cinema (see Table 4-7), for which we suggest two reasons. Firstly, this finding might be a result of a stronger preference for receiving (relevant) information via e-mail than the respondents in the other samples. Secondly, the results could be due to storing email address being the clear status quo for cinema, whereas the other industries have a less homogenous status quo. Therefore, deviating from this status quo might be more influential for cinema compared to the other industries.

With regard to information use, we show that consumers are, on average, not expecting large benefits from personalized insights or personalized marketing content. Prior studies show that consumers are more committed and cooperative when confronted with personalization (e.g., Chung, Wedel, and Rust 2016; Hauser, Liberali, and Urban 2014; Urban

et al. 2013). In our research, we give consumers an evident choice. Describing personalization in the choice context makes it explicit, which could result in reactance (similar as for ads: Aguirre et al. 2015; Bleier and Eisenbeiss 2015a; Van Doorn and Hoekstra 2013; Goldfarb and Tucker 2011). Still, removing personalized marketing content also only has a marginal positive impact on choice probabilities so that firms who are currently using personalized marketing content are not forced to act. Moreover, in contrast to our hypothesis ($H_{2a}$), the benefits of information use are not enhanced by interaction intensity. Thus, even in industries in which consumers interact often with firms they are not expecting benefits from personalized insights or personalized marketing content. Furthermore, our findings confirm that consumers strongly oppose external dissemination of information in any industry (e.g., Wirtz and Lwin 2009). Combining the considerable loss of disclosing sensitive information with the uncertainty of sharing information with third parties repels consumers even more.

We also show that offering control and (to a lesser extent) transparency over the collection, storage, or use of information each have a positive effect on consumers. Transparency and control are more important in industries that are considered sensitive, confirming our hypotheses ($H_{1b}$ and $H_{1c}$), although only at a 10% level. Transparency matters less when consumers interact more frequently with the firm (rejects $H_{2b}$). We believe that when consumers interact less often with a firm they might recall the privacy settings less well, so that transparency becomes more valuable. Overall, offering transparency and control is beneficial because most consumers believe that their current firm provides neither transparency (67%) nor control (59%). As consumers believe they are "*being kept in the dark*" and "*have lost all control*" (TNS 2011), promoting transparency and control represents a promising option for strategic differentiation. The sensitivity analysis confirms that promoting control and (to a lesser extent) transparency motivates consumers to accept information collection. Arguably, adding control is more consequential for firms so that they

**Table 4-8.** Testing of hypotheses

| **Hypothesis** | **Confirmed** |
|---|---|
| $H_{1a}$: The relative importance of information collection is higher when information sensitivity of an industry is high | Confirmed |
| $H_{1b}$: The relative importance of transparency is higher when information sensitivity of an industry is high | Confirmed* |
| $H_{1c}$: The relative importance of control is higher when information sensitivity of an industry is high | Confirmed* |
| $H_{2a}$: The relative importance of information use is higher when interaction intensity of an industry is high | Rejected |
| $H_{2b}$: The relative importance of transparency is higher when interaction intensity of an industry is high | Rejected |
| $H_{2c}$: The relative importance of control is higher when interaction intensity of an industry is high | Rejected |

* Significant at a 10% level

might not be able to collect, store, or use the information as intended. Although the decision to allow control needs to consider this trade off, preliminary evidence suggests that consumers already become more cooperative when they '*feel'* they are in control (Brandimarte, Acquisti, and Loewenstein 2013). Future research should assess whether consumers are indeed not interested in disruption, and thus whether firms would (only) benefit from promising control.

Finally, we show that consumers are, on average, more likely to forego a personalization program than to accept it if this program exhibits a privacy strategy consistent with the current status quo. Accordingly, many strategies result in the majority of consumers

not accepting the personalization program, which stresses the need for firms to improve their privacy strategies or to augment their strategies with other, likely costly, marketing actions.

### 4.6 Limitations and future research

What complicates studying privacy is that consumers might not always pay attention to their privacy. Reviewing privacy statements and terms and conditions is a complex and tedious task for consumers that they typically avoid. Especially in low-involvement (‘*low-effort*’) situations, such as when consumers search online or use their mobile phone, a privacy paradox might occur such that consumers accept information collection in spite of their concerns (Acquisti, Brandimarte, and Loewenstein 2015; Dinev, McConnell, and Smith 2015). Also in our study we cannot rule out that consumers might have used heuristics in order to decide which option to prefer instead of carefully considering all information present (indicated by the non-significant interaction effects, e.g., between control of information collection and information collection elements). We still believe that our setting mimicked reality in which consumers also do not process all the information about privacy available. In this realm, our study identifies which cues consumers take in order make a decision whether to accept information collection or not.

We identify transparency and control as influential privacy elements and show how these elements affect the probability to choose the personalization program. Future research should also address to what extent consumers act upon this opportunity when they are provided with transparency and control, specifically if consumers are in fact controlling the way information is collected, stored, and used. This research stream would allow firms to better understand the consequences of providing transparency and control to consumers.

Furthermore, future research should assess other contextual characteristics that might affect the impact of a firm’s privacy strategy. We show that information sensitivity and, to a lesser extent, interaction intensity moderate the effects. Assessing the acceptance of

information collection in industries that differ on other relevant characteristics would provide highly valuable insights for firms that want to promote privacy.

Moreover, while we searched for the optimal privacy strategy ('*what'*) we do not assess how a firm can promote this strategy to consumers without raising privacy concerns by making it more salient ('*how*'). Specifically, we do not assess whether or how the way firms explain their privacy strategy affects our results. Prior research on message framing has discussed the effectiveness of communicating prevention of losses or risks (Tversky and Kahneman 1981). Also in the context of privacy, consumers considered negative consequences more likely when a firm explained the risks (and benefits) of information disclosure (LaRose and Rifon 2007). Future research should assess the '*how*' of promoting privacy in more detail.

Finally, a high level of heterogeneity remains between individuals that cannot be explained by differences in the industries. Future research should assess cognitive drivers that affect preferences. In this context, also cultural differences should be considered. Besides that consumers from different countries and cultures worry about different issues (e.g., Miltgen and Peyrat-Guillard 2014), prior research has suggested that privacy elements are valued differently between countries. As an example, US consumers considered unauthorized secondary use a minor issue, whereas for Singaporean consumers this was the most important privacy violation when dealing with online retailers (Hann et al. 2007). Our study is based on a sample from the Netherlands, which does not allow these inferences. Given that our findings are consistent with the pre-test based on a US sample, we believe that the focus on just one nation is a minor limitation.

## 4.7 Conclusion

Firms struggle in aligning their privacy strategy with consumer preferences. In this context, we provide valuable insights with regard to how a firm can convince consumers to accept or

adopt products and services contingent on accepting the information collection. We show that consumers take all elements of a firm's privacy strategy into account (information collection, information storage, information use, transparency, control) when deciding to accept information collection. We also explain how industry characteristics affect the influence of these elements. Given the growing relevance of privacy our findings provide timely insights for firms that want to promote their privacy strategy.

## Chapter 5.

# General Discussion

This dissertation looks at the influence of privacy on the field of marketing. While collecting information about consumers has become crucial to firms, it has also made consumers worried about their privacy. Besides that recent privacy legislation has made it easier for consumers to reject information collection, firms that neglect these concerns have been publicly condemned. This has resulted in several marketing scholars stating privacy has become an important topic within marketing (Ferrell 2016; Wedel and Kannan 2016). In order to provide firms some guidance on how to manage consumer privacy our main research question is formulated as follows: *How do firms' privacy practices affect consumers?* Specifically, more understanding is needed under which circumstances consumers are more or less willing to disclose information, and how firms' privacy practices affect consumers. Firms' recent struggles suggest consumer privacy can be a business opportunity for those firms that properly manage consumers' information (Goldfarb and Tucker 2013). In this final chapter we aim to answer our research question by reiterating the key findings from three studies, and based on these findings we end with direction for future research.

## 5.1 Main findings and managerial implications

*Chapter 2* – Despite the growing importance of privacy, a deep understanding of how firms' privacy practices affect consumers remains absent. In chapter two we review the relevant literature on consumer privacy from a marketing perspective and summarize current knowledge about how information collection, information storage, information use, transparency, and control affects consumers' attitudes or perceptions (e.g., privacy concern) and their intentions or behavior (e.g., information disclosure). In addition, we describe to what extent the influence of firms' privacy practices differs between firms, consumers, and environments. Based on a structured overview of the current knowledge we identify knowledge gaps, for which we formulate research propositions aimed at providing direction for future research regarding the role of privacy in marketing.

The key findings from prior studies are that besides any negative consequences (*privacy concern*) consumers also seem to take the positive consequences of information collection into account (*privacy calculus*), although in low-involvement situations consumers can behave inconsistent (*privacy paradox*) with this trade-off. Nevertheless, besides that consumers are affected by '*what*' (e.g., information sensitivity) also '*how*' firms collect information matters, which also influences the responsiveness to (monetary) incentives. Moreover, besides preventing security breaches, which have shown to diminish firm value, the mere promise of safe storage also has a direct positive influence on consumers. While using information for personalization makes consumers more satisfied and committed, too much personalization, in particular in online advertisements, arouses privacy concern. Likewise, while should transparency enhance the relationship between firms and consumers, it can also trigger privacy concern. Communicating how consumers benefit convinces them to accept products and services contingent on information collection. Transparency is most effective in conjunction with control, as promising control makes consumers more cooperative and committed. Finally, for all findings holds that firms need to take into account that the influence of privacy practices differs between firms, consumers, and environments.

For managers this implies that although online and on mobile devices consumers are susceptible for biases and heuristics, consumers usually consider both positive and negative consequences. Therefore, managers need to exercise caution when collecting sensitive information, such as information on consumers' location or their offline behavior, as that intensifies the (potential) negative consequences. Although effective in some situations managers should be tentative in providing monetary incentives for sensitive information. Moreover, besides that firms should make sure their information storage is secure in order to avoid security breaches, emphasizing that only authorized personnel has access or that information is stored locally (i.e., on the device) can also contribute to more committed and

loyal customers. Although consumers have embraced the rise of personalized content, such as websites and advertisements, managers need to be aware that (too much) personalization is considered intrusive. Resolving this issue requires increasing the relevance, as when mobile ads are relevant both in time and location consumers focus more on usefulness than intrusiveness. Finally, transparency could be helpful if managers stress the right benefits. For example, promising free service increases the acceptance of information collection more than stressing enhanced relevance of ads. Furthermore, transparency is most effective when firms also provide control, as otherwise it only accentuates that consumers have no influence on how their information is handled.

*Chapter 3* – In our third chapter we aim to provide a better understanding of when and why consumers accept or reject information collection. Given the discrepancy between privacy concern and behavior (privacy paradox), we focus instead on consumers' internal privacy trade-off (privacy calculus). Besides considering both positive and negative consequences of information collection, storage, and use we take into account that these consequences are not always certain to affect consumers. More specifically, we suggest that the privacy calculus should be based on the perceived valence and probability of different types of consequences (financial, performance, psychological, security, social, time). On the basis of this conceptualization, we develop the PRICAL index, which uses formative items to measure the privacy calculus. Following a qualitative phase, we empirically confirm the validity of the items (Study 1) and the index as a whole (Study 2 and Study 3) in various contexts.

Besides being embedded in theory, the privacy calculus construct and the PRICAL index better explain behavioral intentions and actual behavior than currently used constructs (e.g., privacy concern, trust). The main outcome of this chapter is our measurement tool, which provides a better understanding of the acceptance of information collection. We take a broader perspective as we show that rather than privacy concern consumers are driven by

their internal privacy trade-off, which depends on a wide variety of consequences. Understanding this trade-off requires taking into account that consumers differ in whether they consider consequences positive or negative (valence) and also whether they believe these consequences will affect them (probability).

For firms our findings imply that to understand why consumers accept or reject information collection, managers need to consider a wide variety of tangible and intangible consequences. Moreover, rather than neglecting consequences that managers believe will never happen they need to take consumers' perceived probability of these consequences into account. Managers can use our PRICAL index to better understand the acceptance of products and (added) services that are conditional on collecting information. For example, the PRICAL index explains consumers' willingness to disclose their location to their telecom provider for location-based advertising, and whether they accept that their insurance firm tracks their driving behavior for usage-based insurance.

*Chapter 4* – Firms struggle in aligning their privacy strategy with consumer preferences. As this represents an opportunity for firms to optimize their privacy strategy we look at how managerial decisions with regard to a firm's privacy strategy affect consumers in chapter four. Based on our definition of privacy we discern five main elements of firms' privacy strategy (information collection, information storage, information use, transparency, control) that have shown to affect consumers. Our main objective is to provide insights in which of these privacy elements affects consumers the most, and whether this differs between industries.

To generate these insights we use a choice-based conjoint experiment, in which we assess whether consumers accept a personalization program for which we vary the way information is collected, stored, and used, and the amount of transparency and control over these elements provided by firms. To assure managerial relevance we focus on decisions with regard to these elements that are under managerial control, i.e., things that firms can actually

change. Moreover, to broaden our findings we assess to what extent the influence of these elements differs based on industry characteristics that might enhance the risks (information sensitivity) or the benefits (interaction intensity).

The key insights for managers are that although all privacy elements affect consumers' acceptance of information collection, information collection and use matter more in highly sensitive industries, while storage matters less. More specifically, we show that in these industries managers should be reluctant with regard to collecting and sharing information externally. The influence of interaction intensity is less pronounced, as it has a (relatively) limited impact on the importance of transparency and control. Most importantly, as consumers believe that few firms provide transparency and control, our findings show that firms have much to gain from promising transparency and control.

### 5.2 Future research directions

In this dissertation we introduce the topic of privacy to the field of marketing. The growing importance of collecting information about consumers, for example to enable Customer Relationship Management, Customer Intelligence, and, more recently, one-to-one marketing, combined with the novelty of the topic makes that much work is still to be done.

Firstly, while we partly resolve the privacy paradox by developing a measurement tool for the privacy calculus, future work should assess when the privacy calculus does and when it does not explain behavior. Given the prevalence of the privacy paradox more studies using actual information accepting or rejecting behavior—such as accepting data-driven services, cookies, and apps—should be conducted. Revealing under which circumstances the privacy calculus conflicts with behavior might also inform legislators when they should try and protect consumers more thoroughly. For example, when consumers are unaware about when and how information is collected and used legislators might try to educate consumers. When consumers decide unconsciously or rely on heuristics this might indicate that informed

consent is ineffective, as several scholars have suggested (Landau 2015; Nissenbaum 2015), and that legislators might need to regulate consumers' privacy more extensively.

Secondly, in situations in which the privacy calculus does explain consumers' acceptance of information collection, such as the adoption of data-driven offerings, future work should assess which dimensions of the privacy calculus are most important under which circumstances. Providing these insights would enable firms to emphasize the most important benefits, while preventing the most detrimental consequences.

A third important area for future research is assessing the long-term effect of respecting or ignoring consumers' privacy preferences. Many firms seem to consider keeping consumers in the dark about the collection, storage, and use of information as a viable strategy. Future work should study how consumers respond to a lack of transparency in the long run, and assess how consumers respond when they find out about privacy transgressions, either attitudinal (loss of trust) or behavioral (switch firms, negative WOM).

Fourthly, future research should assess the role of transparency and control more extensively. We show that promising transparency and control positively affects consumers across industries. Future work should assess to what extent consumers actually make use of this, as that could be the (potential) downside for firms. While game-theoretic models suggest that proactive privacy protection is a viable business model (Lee, Ahn, and Bang 2011), whether this also works in practice remains to be seen.

Finally, future work should assess in more detail how the influence of privacy and the main elements of privacy differs between contexts. In line with the theory of contextual integrity (Nissenbaum 2004) we show that industry characteristics, i.e., information sensitivity and interaction intensity, affect the influence of privacy on consumers. Future work should not only assess other industry characteristics, but should also assess to what extent cultural or individual-specific characteristics play a role.

## 5.3 Concluding remarks

The main aim of this dissertation is to assess how privacy affects firms and consumers. Firms have to be aware that besides looking at outcomes (distributive fairness, i.e., information collection, storage, use) consumers also take the way these outcomes come about (procedural fairness, i.e., transparency, control) into account. Moreover, the effect of these privacy elements differs between firms, consumers, and environments.

More specifically, we show when deciding upon the acceptance of products and services contingent on collecting information consumers take the perceived consequences of information collection, storage, and use into account. Rather than looking only at the negative consequences (privacy concerns), we show that in order to better understand consumers one also has to take the positive consequences into account. Besides looking at both sides one also has to take into account that in the eyes of consumers some consequences are more likely to affect them than others, and by taking the perceived probability into account one can better explain why consumers accept information collection.

Moreover, when firms want to align their privacy strategy with consumers' preferences they have to take into account that these preferences differ between industries. More specifically, which element matters most differs based on the status quo in an industry and on whether firms handle very sensitive or insensitive information.

While this dissertation provides a better understanding of how privacy affects firms and consumers, it merely represents a first step. Over the past decade firms have been able to track the behavior of individual consumers online. As the rise of the '*Internet of Things'* continues, firms become able to collect, store, and use information about how consumers behave offline. In response, privacy concerns are expected to surge (Groopman and Etlinger 2015), which will prompt governments to enforce (even) more privacy protection. Therefore, understanding privacy stands to become one of the key strategic issues for firms in the future.

# Chapter 6.

# References

Ackerman, Mark S., Lorrie Faith Cranor, and Joseph Reagle (1999), "Privacy in e-commerce: Examining user scenarios and privacy preferences," *ACM Conference on Electronic Commerce*.

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein (2015), "Privacy and human behavior in the age of information," *Science*, 347 (6221), 509–14.

———, Allan Friedman, and Rahul Telang (2006), "Is there a cost to privacy breaches? An event study," in *WEIS*.

——— and Jens Grossklags (2005a), "Privacy and rationality in individual decision making," *Security & Privacy, IEEE*, 3 (1).

——— and ——— (2005b), "Uncertainty, ambiguity and privacy," in *WEIS*, 1–21.

———, Leslie K. John, and George Loewenstein (2012), "The impact of relative standards on the propensity to disclose," *Journal of Marketing Research*, 49 (2), 160–74.

———, ———, and ——— (2013), "What is privacy worth?," *Journal of Legal Studies*, 42 (2), 249–74.

———, Curtis R. Taylor, and Liad Wagman (2016), "The economics of privacy," *Journal of Economic Literature*, 54 (2), 442–92.

——— and Hal R. Varian (2005), "Conditioning prices on purchase history," *Marketing Science*, 24 (3), 367–81.

Adjerid, Idris, Alessandro Acquisti, Rahul Telang, Rema Padman, and Julia Adler-Milstein (2016), "The impact of privacy regulation and technology incentives: The case of health information exchanges," *Management Science*, ((Forthcoming)).

Adomavicius, Gediminas and Alexander Tuzhilin (2005), "Personalization technologies,"

*Communications of the ACM*, 48 (10), 83–90.

Aguirre, Elizabeth, Dominik Mahr, Dhruv Grewal, Ko de Ruyter, and Martin Wetzels (2015), "Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness," *Journal of Retailing*, 91 (1), 34–49.

Aiken, K. Damon and David M. Boush (2006), "Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of internet signals," *Journal of the Academy of Marketing Science*, 34 (3), 308–23.

Aljukhadar, Muhammad, Sylvain Senecal, and Denis Ouellette (2010), "Can the media richness of a privacy disclosure enhance outcome? A multifaceted view of trust in rich media environments," *International Journal of Electronic Commerce*, 14 (4), 103–26.

Alreck, Pamela L. and Robert B. Settle (2007), "Consumer reactions to online behavioural tracking and targeting," *Journal of Database Marketing & Customer Strategy Management*, 15 (1), 11–23.

Altman, Irwin (1975), *The environment and social behavior: Privacy, personal space, territory, and crowding*, Monterey, CA: Brooks/Cole Publishing.

Andrade, Eduardo B., Velitchka Kaltcheva, and Barton Weitz (2002), "Self-disclosure on the web: The impact of privacy policy, reward, and company reputation," *Advances in Consumer Research*, 29, 350–54.

Ansari, Asim and Carl F. Mela (2003), "E-Customization," *Journal of Marketing Research*, 40 (2), 131–45.

Ariely, Dan (2009), "The end of rational economics," *Harvard Business Review*, July-Aug.

Ashley, Christy, Stephanie M. Noble, Naveen Donthu, and Katherine N. Lemon (2011), "Why customers won't relate: Obstacles to relationship marketing engagement," *Journal of Business Research*, 64 (7), 749–56.

Athey, Susan, Christian Catalini, and Catherine E. Tucker (2017), "The digital privacy paradox: Small money, small costs, small talk," *Working Paper*.

Awad, Naveen Farag and M. S. Krishnan (2006), "The personalization privacy paradox : An empirical evaluation of information transparency and the willingness to be profiled online for personalization," *MIS Quarterly*, 30 (1), 13–28.

Bagozzi, Richard P. (2011), "Measurement and meaning in information systems and organizational research: Methodological and philosophical foundations," *MIS Quarterly*, 35 (2), 261–92.

Bansal, Gaurav, Fatemeh Mariam Zahedi, and David Gefen (2008), "The moderating influence of privacy concern on the efficacy of privacy assurance mechanisms for building trust: A multiple-context investigation," in *ICIS 2008 Proceedings*, 1–20.

———, ———, and ——— (2010), "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online," *Decision Support Systems*, 49 (2), 138–50.

———, ———, and ——— (2015), "Do context and personality matter? Trust and privacy concerns in disclosing private information online," *Information & Management*, 53 (1), 1–21.

Bart, Yakov, Venkatesh Shankar, Fareena Sultan, and Glen L. Urban (2005), "Are the drivers

and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study," *Journal of Marketing*, 69 (4), 133–52.

Bauer, Raymond A. (1960), "Consumer behavior as risk taking," in *Dynamic marketing for a changing world*, R. S. Hancock, ed., Chicago: American Marketing Association, 389–98.

Belanger, France, Janine S. Hiller, and Wanda J. Smith (2002), "Trustworthiness in electronic commerce: The role of privacy, security, and site attributes," *Journal of Strategic Information Systems*, 11, 245–70.

Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse (2004), "International differences in information privacy concerns: A global survey of consumers," *The Information Society*, 20 (5), 313–24.

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann (2005), "Privacy in e-commerce," *Communications of the ACM*, 48 (4), 101–6.

Bleier, Alexander and Maik Eisenbeiss (2015a), "Personalized online advertising effectiveness: The interplay of what, when, and where," *Marketing Science*, 34 (5), 669–88.

——— and ——— (2015b), "The importance of trust for personalized online advertising," *Journal of Retailing*, 91 (3), 390–409.

Bloomberg (2016), "2016 was a record year for data breaches," *[Accessed on: 28-08-2017]*.

Bolderdijk, Jan Willem, Linda Steg, and Tom Postmes (2013), "Fostering support for work floor energy conservation policies: Accounting for privacy concerns," *Journal of Organizational Behavior*, 34 (2), 195–210.

Bollen, Kenneth A. (1984), "Multiple indicators: Internal consistency or no necessary

relationship?," *Quality and Quantity*, 18 (4), 377–85.

——— and Richard Lennox (1991), "Conventional wisdom on measurement: A structural equation perspective," *Psychological Bulletin*, 110 (2), 305–14.

Bolton, Ruth N. and Shruti Saxena-Iyer (2009), "Interactive services: A framework, synthesis and research directions," *Journal of Interactive Marketing*, 23 (1), 91–104.

Borsboom, Denny, Gideon J. Mellenbergh, and Jaap Van Heerden (2004), "The concept of validity," *Psychological Review*, 111 (4), 1061–71.

Boulding, William and Amna Kirmani (1993), "A consumer-side experimental examination of signaling theory: Do consumers perceive warranties as signals of quality?," *Journal of Consumer Research*, 20 (1), 111–23.

———, Richard Staelin, Michael Ehret, and Wesley J. Johnston (2005), "A customer relationship management roadmap: What is known, potential pitfalls, and where to go," *Journal of Marketing*, 69 (4), 155–66.

Bowen, John (1990), "Development of a taxonomy of services to gain strategic marketing insights," *Journal of the Academy of Marketing Science*, 18 (1), 43–49.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein (2013), "Misplaced confidences: Privacy and the control paradox," *Social Psychological and Personality Science*, 4 (3), 340–47.

Brazell, Jeff D., Christopher G. Diener, Ekaterina Karniouchina, William L. Moore, Valerie Severin, and Pierre Francois Uldry (2006), "The no-choice option and dual response choice designs," *Marketing Letters*, 17 (4), 255–68.

Brehm, Jack W. (1966), *A theory of psychological reactance*, Oxford, England: Academic

Press.

BTG (2012), "KPN introduceert Nederlandse clouddienst," *[Accessed on: 28-08-2017]*.

Burgoon, Judee K., Roxanne Parrott, Bethe A. Le Poire, Douglas L. Kelley, Joseph B. Walther, and Denise Perry (1989), "Maintaining and restoring privacy through communication in different types of relationships," *Journal of Social and Personal Relationships*, 6 (2), 131–58.

Caudill, Eve M. and Patrick E. Murphy (2000), "Consumer online privacy: Legal and ethical issues," *Journal of Public Policy & Marketing*, 19 (1), 7–19.

Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan (2004), "The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers," *International Journal of Electronic Commerce*, 9 (1), 69–104.

Cenfetelli, Ronald T. and Geneviève Bassellier (2009), "Interpretation of the formative measurement in information systems research," *MIS Quarterly*, 33 (4), 689–707.

Chaiken, Shelly (1980), "Heuristic Versus Systematic Information Processing and the Use of Source Versus Message Cues in Persuasion," *Journal of Personality and Social Psychology*, 39 (5), 752–66.

Chellappa, Ramnath K. and Raymond G. Sin (2005), "Personalization versus privacy: An empirical examination of the online consumer's dilemma," *Information Technology and Management*, 6, 181–202.

Chung, Tuck Siong, Roland T. Rust, and Michel Wedel (2009), "My mobile music: An adaptive personalization system for digital audio players," *Marketing Science*, 28 (1),

52–68.

———, Michel Wedel, and Roland T. Rust (2016), "Adaptive personalization using social networks," *Journal of the Academy of Marketing Science*, 44 (1), 66–87.

Churchill Jr., Gilbert A. (1979), "A paradigm for developing better measures of marketing constructs," *Journal of Marketing Research*, 16 (1), 64–73.

CIGI-Ipsos (2017), "Global Survey on Internet Security and Trust."

CNN (2005), "Web sites change prices based on customers' habits," *[Accessed on: 28-08-2017]*.

Coelho, Pedro S. and Jörg Henseler (2012), "Creating customer loyalty through service customization," *European Journal of Marketing*, 46 (3/4), 331–56.

Conchar, Margy P., George M. Zinkhan, Cara Peters, and Sergio Olavarrieta (2004), "An integrated framework for the conceptualization of consumers' perceived-risk processing," *Journal of the Academy of Marketing Science*, 32 (4), 418–36.

Culnan, Mary J. (1993), "' How did they get my name?': An exploratory investigation of consumer attitudes toward secondary information use," *MIS Quarterly*, 17 (3), 341–63.

——— (1995), "Consumer awareness of name removal procedures: Implications for direct marketing," *Journal of Direct Marketing*, 9 (2), 10–19.

——— and Pamela K. Armstrong (1999), "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation," *Organization Science*, 10 (1), 104–15.

——— and Robert J. Bies (2003), "Consumer privacy: Balancing economic and justice considerations," *Journal of Social Issues*, 59 (2), 323–42.

Cunningham, Scott M. (1967), "The major dimensions of perceived risk," in *Risk taking and information handling in consumer behavior*, D. F. Cox, ed., Boston: Harvard University Press, 82–108.

Danaher, Peter J., Denise M. Conroy, and Janet R. McColl-Kennedy (2008), "Who wants a relationship anyway?," *Journal of Service Research*, 11 (1), 43–62.

Davis, Fred D. (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS Quarterly*, 13 (3), 319–40.

Deloitte (2014), "Building consumer trust: Protecting personal data in the consumer product industry."

Demoulin, Nathalie T. M. and Pietro Zidda (2009), "Drivers of customers' adoption and adoption timing of a new loyalty card in the grocery retail market," *Journal of Retailing*, 85 (3), 391–405.

Derikx, Sebastian, Mark de Reuver, and Maarten Kroesen (2016), "Can privacy concerns for insurance of connected cars be compensated?," *Electronic Markets*, 26 (1), 73–81.

Devaraj, Sarv, Robert F. Easley, and J. Michael Crant (2008), "Personality matter? Relating the five-factor model to technology acceptance," *Information Systems Research*, 19 (1), 93–105.

Diamantopoulos, Adamantios, Petra Riefler, and Katharina P. Roth (2008), "Advancing formative measurement models," *Journal of Business Research*, 61 (12), 1203–18.

——— and Heide M. Winklhofer (2001), "Index construction with formative indicators: An alternative to scale development," *Journal of Marketing Research*, 38 (2), 269–77.

Dick, Alan S. and Kunal Basu (1994), "Customer loyalty: Toward an integrated conceptual

framework," *Journal of the Academy of Marketing Science*, 22 (2), 99–113.

Dinev, Tamara and Paul Hart (2006), "An extended privacy calculus model for e-commerce transactions," *Information Systems Research*, 17 (1), 61–80.

———, Allen R. McConnell, and Jeff H. Smith (2015), "Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the 'APCO' box," *Information Systems Research*, 26 (4), 639–55.

———, Heng Xu, Jeff H. Smith, and Paul Hart (2013), "Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts," *European Journal of Information Systems*, 22 (3), 295–316.

Dolnicar, Sara and Yolanda Jordaan (2007), "A market-oriented approach to responsibility managing information privacy concerns in direct marketing," *Journal of Advertising*, 36 (2), 123–49.

Donaldson, Thomas and Thomas W. Dunfee (1994), "Towards a unified conception of business ethics: Integrative social contracts theory," *Academy of Management Review*, 19 (2), 252–84.

Van Doorn, Jenny and Janny C. Hoekstra (2013), "Customization of online advertising: The role of intrusiveness," *Marketing Letters*, 24 (4), 339–51.

Dorotic, Matilda, Tammo H.A. Bijmolt, and Peter C. Verhoef (2012), "Loyalty programmes: Current knowledge and research directions," *International Journal of Management Reviews*, 14 (3), 217–37.

Dowling, Grahame R. (1986), "Perceived risk: The concept and its measurement," *Psychology & Marketing*, 3 (3), 193–210.

Eastlick, Mary Ann, Sherry L. Lotz, and Patricia Warrington (2006), "Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment," *Journal of Business Research*, 59 (8), 877–86.

Edwards, Steven M., Hairong Li, and Joo-Hyun Lee (2002), "Forced exposure and psychological reactance: Antecedents and consequences of the perceived intrusiveness of pop-up ads," *Journal of Advertising*, 31 (3), 83–95.

Eurobarometer (2011), "Attitudes on data protection and electronic identity in the European Union."

Farrell, Joseph (2012), "Can privacy be just another good?," *Journal on Telecommunication & High Technology Law*, 10, 251–61.

Fazio, Russell H., Martha C. Powell, and Carol J. Williams (1989), "The Role of Attitude Accessibility in the Attitude-to-Behavior Process," *Journal of Consumer Research*, 16 (3), 280–88.

Featherman, Mauricio S., Anthony D. Miyazaki, and David E. Sprott (2010), "Reducing online privacy risk to facilitate e-service adoption: The influence of perceived ease of use and corporate credibility," *Journal of Services Marketing*, 24 (3), 219–29.

Feinberg, Fred M., Aradhna Krishna, and Z. John Zhang (2002), "Do we care what others get? A behaviorist approach to targeted promotions," *Journal of Marketing Research*, 39 (3), 277–91.

Ferrell, O. C. (2016), "Broadening marketing's contribution to data privacy," *Journal of the Academy of Marketing Science*, 45 (2), 160–63.

Fishbein, Martin and Icek Ajzen (1975), *Belief, attitude, intention, and behavior: An*

*introduction to Theory and Research*, Reading, MA: Addition-Wesley.

Forbes (2013), "How Nordstrom uses WiFi to spy on shoppers," *[Accessed on: 28-08-2017]*.

——— (2015), "Samsung's smart TVs share living room conversations with third parties," *[Accessed on: 28-08-2017]*.

Foxman, Ellen R. and Paula Kilcoyne (1993), "Information technology, marketing practice, and consumer privacy: Ethical issues," *Journal of Public Policy & Marketing*, 12 (1), 106–19.

Frow, Pennie, Adrian Payne, Ian F. Wilkinson, and Louise Young (2011), "Customer management and CRM: Addressing the dark side," *Journal of Services Marketing*, 25 (2), 79–89.

Gabisch, Jason Aaron and George R. Milne (2014), "The impact of compensation on information ownership and privacy control," *Journal of Consumer Marketing*, 31 (1), 13–26.

General Data Protection Regulation (EU) (2018), *General Data Protection Regulation*, European Commission.

Gerbing, David W. and James C. Anderson (1988), "An updated paradigm for scale development incorporating unidimensionality and its assessment," *Journal of Marketing Research*, 25 (2), 186–92.

Goldfarb, Avi and Catherine E. Tucker (2011a), "Privacy regulation and online advertising," *Management Science*, 57 (1), 57–71.

——— and ——— (2011b), "Online display advertising: Targeting and obtrusiveness," *Marketing Science*, 30 (3), 389–404.

——— and ——— (2012), “Shifts in privacy concerns,” *American Economic Review*, 102 (3), 349–53.

——— and ——— (2013), “Why managing customer privacy can be an opportunity,” *MIT Sloan Management Review*, 54 (3).

Goodwin, Cathy (1991), “Privacy: Recognition of a consumer right,” *Journal of Public Policy & Marketing*, 10 (1), 149–66.

Gosling, Samuel D., Peter J. Rentfrow, and William B. Swann (2003), “A very brief measure of the Big-Five personality domains,” *Journal of Research in Personality*, 37 (6), 504–28.

Groopman, Jessica and Susan Etlinger (2015), “Consumer perceptions of privacy in the Internet of Things.”

Gurau, Calin and Ashok Ranchhod (2009), “Consumer privacy issues in mobile commerce: A comparative study of British, French and Romanian consumers,” *Journal of Consumer Marketing*, 26 (7), 496–507.

Hair, Joseph F., G. Tomas M. Hult, Christian M. Ringle, and Marko Sarstedt (2014), *A primer on partial least squares structural equation modeling (PLS-SEM)*, Thousand Oaks (CA): SAGE Publications.

———, G. Tomas M Hult, Christian M. Ringle, Marko Sarstedt, and Kai Oliver Thiele (2017), “Mirror, mirror on the wall: A comparative evaluation of composite-based structural equation modeling methods,” *Journal of the Academy of Marketing Science*, Online Fir (February), 1–17.

Hann, Il-Horn, Kai-lung Hui, Tom S. Lee, and Ivan P. L. Png (2007), “Overcoming online

information privacy concerns: An information-processing theory approach," *Journal of Management Information Systems*, 24 (2), 13–42.

Hardesty, David M. and William O. Bearden (2004), "The use of expert judges in scale development," *Journal of Business Research*, 57 (2), 98–107.

Hauser, John R. (1978), "Testing the accuracy, usefulness, and significance of probabilistic choice models: An information-theoretic approach," *Operations Research*, 26 (3), 406–21.

———, Guilherme Liberali, and Glen L. Urban (2014), "Website morphing 2.0: Switching costs, partial exposure, random exit, and when to morph," *Management Science*, 60 (6), 1594–1616.

———, Glen L. Urban, Guilherme Liberali, and Michael Braun (2009), "Website morphing," *Marketing Science*, 28 (2), 202–23.

Heckman, J. (1979), "Sample selection bias as a specification error," *Econometrica*, 47 (1), 153–61.

Heimbach, Irina, Jörg Gottschlich, and Oliver Hinz (2015), "The value of user's Facebook profile data for product recommendation generation," *Electronic Markets*, 25 (2), 125–38.

Hennig-Thurau, Thorsten, Kevin P. Gwinner, and Dwayne D. Gremler (2002), "Understanding relationship marketing outcomes: An integration of relational benefits and relationship quality," *Journal of Service Research*, 4 (3), 230–47.

Henseler, Jörg, Theo K. Dijkstra, Marko Sarstedt, Christian M. Ringle, Adamantios Diamantopoulos, Detmar W. Straub, David J. Ketchen, Joseph F. Hair, G. Tomas M.

Hult, and Roger J. Calantone (2014), "Common beliefs and reality about PLS: Comments on Ronkko and Evermann (2013)," *Organizational Research Methods*, 17 (2), 182–209.

———, Christian M. Ringle, and Rudolf R. Sinkovics (2009), "The use of partial least squares path modeling in international marketing," *Advances in International Marketing*, 20, 177–91.

Hermalin, Benjamin E. and Michael L. Katz (2006), "Privacy, property rights and efficiency: The economics of privacy as secrecy," *Quantitative Marketing and Economics*, 4 (3), 209–39.

Higgins, E. Tory (1997), "Beyond pleasure and pain," *American Psychologist*, 52 (12), 1280–1300.

Hille, Patrick, Gianfranco Walsh, and Mark Cleveland (2015), "Consumer fear of online identity theft: Scale development and validation," *Journal of Interactive Marketing*, 30 (May), 1–19.

Hinkin, Timothy R. (1995), "A review of scale development practices in the study of organizations," *Journal of Management*, 21 (5), 967–88.

Hoffman, Donna L., Thomas P. Novak, and Marcos Peralta (1999), "Building consumer trust online," *Communications of the ACM*, 42 (4).

Hogan, John E., Katherine N. Lemon, and Roland T. Rust (2002), "Customer equity management: Charting new directions for the future of marketing," *Journal of Service Research*, 5 (1), 4–12.

Holtrop, Niels, Jaap E. Wieringa, Maarten J. Gijsenberg, and Peter C. Verhoef (2017), "No

future without the past? Predicting churn in the face of customer privacy," *International Journal of Research in Marketing*, 34 (1), 154–72.

Homans, George C. (1958), "Social behavior as exchange," *American Journal of Sociology*, 63 (6), 597–606.

Hong, Weiyin and James Y. L. Thong (2013), "Internet privacy concerns: An integrated conceptualization and four empirical studies," *MIS Quarterly*, 37 (1), 275–98.

Hoofnagle, Chris Jay and Jennifer M. Urban (2014), *Alan Westin's Privacy Homo Economicus*.

Huber, Joel and Klaus Zwerina (1996), "The importance of utility balance in efficient choice designs," *Journal of Marketing Research*, 33 (3), 307–17.

Huffington Post (2017), "Smart speakers and voice recognition: Is your privacy at risk?," *[Accessed on: 28-08-2017]*.

Hui, Kai-Lung, Hock-Hai Teo, and Tom S. Lee (2007), "The value of privacy assurance: An exploratory field experiment," *MIS Quarterly*, 31 (1), 19–33.

Jacoby, Jacob and Leon B. Kaplan (1972), "The components of perceived risk," in *Proceedings of the Third Annual Conference of the Association for Consumer Research*, M. Venkatesan, ed., Chicago, IL, 382–93.

Jai, Tun-Min (Catherine), Leslie Davis Burns, and Nancy J. King (2013), "The effect of behavioral tracking practices on consumers' shopping evaluations and repurchase intention toward trusted online retailers," *Computers in Human Behavior*, 29 (3), 901–9.

Jarvis, Cheryl Burke, Scott B. MacKenzie, and Philip M. Podsakoff (2003), "A critical review of construct indicators and measurement model misspecification in marketing and

consumer research," *Journal of Consumer Research*, 30 (2), 199–218.

Jiang, Zhenhui (Jack), Cheng Suang Heng, and Ben C. F. Choi (2013), "Research Note - Privacy concerns and privacy-protective behavior in synchronous online social interactions," *Information Systems Research*, 24 (3), 579–95.

John, Leslie K. (2015), "We say we want privacy online, but our actions say otherwise," *Harvard Business Review*.

———, Alessandro Acquisti, and George Loewenstein (2011), "Strangers on a plane: Context-dependent willingness to divulge sensitive information," *Journal of Consumer Research*, 37 (5), 858–73.

Johnson, Eric J., Steven Bellman, and Gerald L. Lohse (2002), "Defaults, framing and privacy: Why opting in-opting out," *Marketing Letters*, 13 (1), 5–15.

Joinson, Adam N., Ulf-Dietrich Reips, Tom Buchanan, and Carina B. Paine Schofield (2010), "Privacy, trust, and self-disclosure online," *Human-Computer Interaction*, 25 (1), 1–24.

Junglas, Iris A., Norman A. Johnson, and Christiane Spitzmüller (2008), "Personality traits and concern for privacy: An empirical study in the context of location-based services," *European Journal of Information Systems*, 17 (4), 387–402.

Kannan, P. K. and Praveen K. Kopalle (2001), "Dynamic pricing on the Internet: Importance and implications for consumer behavior," *International Journal of Electronic Commerce*, 5 (3), 63–83.

Kaplan, Leon B., George J. Szybillo, and Jacob Jacoby (1974), "Components of perceived risk in product purchase," *Journal of Applied Psychology*, 59 (3), 287–91.

Khan, Romana, Michael Lewis, and Vishal Singh (2009), "Dynamic customer management

and the value of one-to-one marketing," *Marketing Science*, 28 (6), 1063–79.

Kim, Dan J., Donald L. Ferrin, and H. Raghav Rao (2009), "Trust and satisfaction, two stepping stones for successful e-commerce relationships: A longitudinal exploration," *Information Systems Research*, 20 (2), 237–57.

Kim, Kyongseok and Jooyoung Kim (2011), "Third-party privacy certification as an online advertising strategy: An investigation of the factors affecting the relationship between third-party certification and initial trust," *Journal of Interactive Marketing*, 25 (3), 145–58.

King, Jennifer (2014), "Taken out of context: An empirical analysis of Westin's privacy scale," in *Symposium on Usable Privacy and Security (SOUPS)*, 1–8.

Klein, Richard and Arun Rai (2009), "Interfirm strategic information flows in logistics supply chain relationships," *MIS Quarterly*, 33 (4), 735–62.

Knijnenburg, Bart P. and Alfred Kobsa (2013), "Making decisions about privacy: Information disclosure in context-aware recommender systems," in *ACM Transactions on Interactive Intelligent Systems*, 1–33.

———, ———, and Hongxia Jin (2013), "Dimensionality of information disclosure behavior," *International Journal of Human Computer Studies*, 71 (12), 1144–62.

Korzaan, Melinda L. and Katherine T. Boswell (2008), "The influence of personality traits and information privacy concerns on behavioral intentions," *Journal of Computer Information Systems*, 48 (4), 15–24.

Krafft, Manfred, Christine M. Arden, and Peter C. Verhoef (2017), "Permission marketing and privacy concerns — Why do customers (not) grant permissions?," *Journal of*

*Interactive Marketing*, 39 (August), 39–54.

Kumaraguru, Ponnurangam and Lorrie Faith Cranor (2005), "Privacy indexes: A survey of Westin's studies," *Technical Report*.

Lacey, Russell, Jaebeom Suh, and Robert M. Morgan (2007), "Differential effects of preferential treatment levels on relational outcomes," *Journal of Service Research*, 9 (3), 241–56.

Lambrecht, Anja and Catherine E. Tucker (2013), "When does retargeting work? Information specificity in online advertising," *Journal of Marketing Research*, 50 (5), 561–76.

Landau, Susan (2015), "Control use of data to protect privacy," *Science*, 347, 504–6.

Lanier, Clinton D. and Amit Saini (2008), "Understanding consumer privacy: A review and future directions," *Academy of Marketing Science Review*, 12 (2).

LaRose, Robert and Nora J. Rifon (2007), "Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior," *Journal of Consumer Affairs*, 41 (1), 127–50.

Larson, Jeffry H. and Nancy J. Bell (1988), "Need for privacy and it's effect upon interpersonal attraction and interaction," *Journal of Social and Clinical Psychology*, 6 (1), 1–10.

Laufer, Robert S. and Maxine Wolfe (1977), "Privacy as a concept and a social issue: A multidimensional developmental theory," *Journal of Social Issues*, 33 (3).

Lee, Dong-Joo, Jae-Hyeon Ahn, and Youngsok Bang (2011), "Managing consumer privacy concerns in personalization: A strategic analysis of privacy protection," *MIS Quarterly*, 35 (2), 423–44.

Leenheer, Jorna, Harald J. Van Heerde, Tammo H.A. Bijmolt, and Ale Smidts (2007), "Do loyalty programs really enhance behavioral loyalty? An empirical analysis accounting for self-selecting members," *International Journal of Research in Marketing*, 24 (1), 31–47.

Li, Hairong, Steven M. Edwards, and Joo-Hyun Lee (2002), "Measuring the intrusiveness of advertisements: Scale development and validation," *Journal of Advertising*, 31 (2), 37–47.

Li, Han, Rathindra Sarathy, and Heng Xu (2010), "Understanding situational online information disclosure as a privacy calculus," *Journal of Computer Information Systems*, 51 (1), 1–29.

Lowry, Paul Benjamin, Jinwei Cao, and Andrea Everard (2011), "Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: The case of instant messaging in two cultures," *Journal of Management Information Systems*, 27 (4), 163–200.

Lu, Yin, Bernard Tan, and Kai-Lung Hui (2004), "Inducing Customers to Disclose Personal Information to Internet Businesses with Social Adjustment Benefits," *Icis*, 571–82.

Luo, Xueming, Michelle Andrews, Zheng Fang, and Chee Wei Phang (2014), "Mobile targeting," *Marketing Science*, 60 (7), 1738–56.

Lwin, May O., Jochen Wirtz, and Andrea J. S. Stanaland (2016), "The privacy dyad," *Internet Research*, 26 (4), 919–41.

———, ———, and Jerome D. Williams (2007), "Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective," *Journal of the Academy of Marketing Science*, 35 (4), 572–85.

MacKenzie, Scott B. and Philip M. Podsakoff (2012), "Common method bias in marketing: Causes, mechanisms, and procedural remedies," *Journal of Retailing*, 88 (4), 542–55.

———, ———, and Nathan P. Podsakoff (2011), "Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques," *MIS Quarterly*, 35 (2), 293–334.

Malhotra, Arvind and Claudia Kubowicz Malhotra (2011), "Evaluating customer information breaches as service failures: An event study approach," *Journal of Service Research*, 14 (1), 44–59.

Malhotra, Naresh K., Sung S. Kim, and James Agarwal (2004), "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," *Information Systems Research*, 15 (4), 336–55.

Marcati, Alberto, Gianluigi Guido, and Alessandro M. Peluso (2008), "The role of SME entrepreneurs' innovativeness and personality in the adoption of innovations," *Research Policy*, 37 (9), 1579–90.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier (2017), "Data privacy: Effects on customer and firm performance," *Journal of Marketing*, 81 (1), 36–58.

——— and Patrick E. Murphy (2017), "The role of data privacy in marketing," *Journal of the Academy of Marketing Science*, 45 (2), 135–55.

Martin, Kirsten E. and Helen Nissenbaum (2016a), "Measuring privacy: Using context to expose confounding variables," *Columbia Science and Technology Law Review*, 18 (176), 1–40.

——— and ——— (2016b), "Measuring privacy: An empirical test using context to expose

confounding variables," *Columbia Science and Technology Law Review*, 18 (Fall), 176–2018.

Mason, Richard O. (1986), "Four ethical issues of the information age," *MIS Quarterly*, 10 (1), 5–12.

McCrae, Robert R. and Paul T. Costa Jr. (1987), "Validation of the five-factor model of personality across instruments and observers.," *Journal of Personality and Social Psychology*, 52 (1), 81–90.

McDonald, Aleecia M. and Lorrie Faith Cranor (2008), "The cost of reading privacy policies," *Journal of Law and Policy for the Information Society*, 4 (3), 540–65.

McKnight, D. Harrison, Vivek Choudhury, and Carhles Kacmar (2002), "Developing and validating trust measures for e-commerce: An integrative typology," *Information Systems Research*, 13 (3), 334–59.

Metzger, Miriam J. (2007), "Communication privacy management in electronic commerce," *Journal of Computer Mediated Communication*, 12 (2), 1–27.

Milberg, Sandra J., Jeff H. Smith, and Sandra J. Burke (2000), "Information privacy: Corporate management and national regulation," *Organization Science*, 11 (1), 35–57.

Miller, Amalia R. and Catherine E. Tucker (2009), "Privacy protection and technology diffusion: The case of electronic medical records," *Management Science*, 55 (7), 1077–93.

Milne, George R. and Maria-Eugenia Boza (1999), "Trust and concern in consumers' perceptions of marketing information management practices," *Journal of Interactive Marketing*, 13 (1), 5–24.

——— and Mary J. Culnan (2004), "Strategies for reducing online privacy risks: Why consumers read (or don't read) online privacy notices," *Journal of Interactive Marketing*, 18 (3), 15–29.

——— and Mary Ellen Gordon (1993), "Direct mail privacy-efficiency trade-offs within an implied social contract framework," *Journal of Public Policy & Marketing*, 12 (2), 206–15.

———, George Pettinico, Fatima M. Hajjat, and Ereni Markos (2017), "Information sensitivity typology: Mapping the degree and type of risk consumers perceive in personal data sharing," *Journal of Consumer Affairs*, 51 (1), 133–61.

Miltgen, Caroline Lancelot and Dominique Peyrat-Guillard (2014), "Cultural and generational influences on privacy concerns: A qualitative study in seven European countries," *European Journal of Information Systems*, 23 (2), 103–25.

Mithas, Sunil, M. S. Krishnan, and Claes Fornell (2005), "Why do customer relationship management applications affect customer satisfaction?," *Journal of Marketing*, 69 (4), 201–9.

Mittal, Banwari (1989), "Measuring purchase-decision involvement," *Psychology & Marketing*, 6 (2), 147–62.

Montgomery, Alan L. and Michael D. Smith (2009), "Prospects for personalization on the Internet," *Journal of Interactive Marketing*, 23 (2), 130–37.

Moon, Youngme (2000), "Intimate exchanges: Using computers to elicit self-disclosure from consumers," *Journal of Consumer Research*, 26 (4), 323–39.

Morgan, Robert M. and Shelby D. Hunt (1994), "The commitment-trust theory of relationship

marketing," *Journal of Marketing*, 58 (3), 20–38.

Mosteller, Jill and Amit Poddar (2017), "To share and protect: Using regulatory focus theory to examine the privacy paradox of consumers' social media engagement and online privacy protection behaviors," *Journal of Interactive Marketing*, 39 (August), 27–38.

Mothersbaugh, David L., William K. Foxx, Sharon E. Beatty, and Sijun Wang (2012), "Disclosure antecedents in an online service context: The role of sensitivity of information," *Journal of Service Research*, 15 (1), 76–98.

Murray, Keith B. and John L. Schlacter (1990), "The impact of services versus goods on consumers' assessment of perceived risk and variability," *Journal of the Academy of Marketing Science*, 18 (1), 51–65.

Murthi, B. P. S. and Sumit Sarkar (2003), "The role of the management sciences in research on personalization," *Management Science*, 49 (10), 1344–62.

Nissenbaum, Helen (2004), "Privacy as contextual integrity," *Washington Law Review*, 79 (1), 101–39.

——— (2011), "A contextual approach to privacy online," *Daedalus*, 140 (4), 32–48.

——— (2015), "Respecting context to protect privacy: Why meaning matters," *Science and Engineering Ethics*.

Norberg, Patricia a. and Daniel R. Horne (2014), "Coping with information requests in marketing exchanges: An examination of pre-post affective control and behavioral coping," *Journal of the Academy of Marketing Science*, 42 (4), 415–29.

Norberg, Patricia A., Daniel R. Horne, and David A. Horne (2007), "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer*

*Affairs*, 41 (1), 100–127.

Nowak, Glen J. and Joseph E. Phelps (1995), "Direct marketing and the use of individual-level consumer information: Determining how and when 'privacy' matters," *Journal of Direct Marketing*, 9 (3), 46–60.

NU.nl (2014), "ING houdt privacygevoelige proef met klantgegevens," *[Accessed on: 28-08-2017]*.

Nunnally, Jum C. and Ira H. Bernstein (1994), "The assessment of reliability," *Psychometric theory*, 3 (1), 248–92.

Ohlhausen, Maureen K. (2014), "Privacy challenge and opportunities: The role of the Federal Trade Commission," *Journal of Public Policy & Marketing*, 33 (1), 4–9.

Olmstead, Kenneth and Michelle Atkinson (2015), "Apps permissions in the Google Play Store," *Pew Research*.

Pan, Yue and George M. Zinkhan (2006), "Exploring the impact of online privacy disclosures on consumer trust," *Journal of Retailing*, 82 (4), 331–38.

Parasuraman, A., Valarie A. Zeithaml, and Arvind Malhotra (2005), "E-S-QUAL: A multiple-item scale for assessing electronic service quality," *Journal of Service Research*, 7 (3), 213–33.

Pavlou, Paul A. (2011), "State of the information privacy literature: where are we and where should we go?," *MIS Quarterly*, 35 (4), 977–88.

Peltier, James W., George R. Milne, and Joseph E. Phelps (2009), "Information privacy research: Framework for integrating multiple publics, information channels, and responses," *Journal of Interactive Marketing*, 23 (2), 191–205.

Peter, J. Paul and Michael J. Ryan (1976), "An investigation of perceived risk at the brand level," *Journal of Marketing Research*, 13 (2), 184–88.

——— and Lawrence X. Tarpey (1975), "A comparative analysis of three consumer decision strategies," *Journal of Consumer Research*, 2 (1), 29–37.

Petronio, Sandra (1991), "Communication boundary management: A theoretical model of managing disclosure of private information between marital couples," *Communication Theory*, 1 (4), 311–35.

Petty, Richard E. and John T. Cacioppo (1986), "The elaboration likelihood model of persuasion," *Advances in Experimental Social Psychology*, 19, 123–205.

Phelps, Joseph E., Glen J. Nowak, and Elizabeth Ferrell (2000), "Privacy concerns and consumer willingness to provide personal information," *Journal of Public Policy & Marketing*, 19 (1), 27–41.

Podsakoff, Philip M., Scott B. MacKenzie, Jeong-Yeon Lee, and Nathan P. Podsakoff (2003), "Common method biases in behavioral research: a critical review of the literature and recommended remedies.," *Journal of Applied Psychology*, 88 (5), 879–903.

Posner, Richard A. (1978), "An economic theory of privacy," *Georgia Law Review*, (May/June), 19–26.

——— (1981), "The economics of privacy," *The American Economic Review*, 71 (2), 405–9.

Premazzi, Katia, Sandro Castaldo, Monica Grosso, Pushkala Raman, Susan Brudvig, and Charles F. Hofacker (2010), "Customer information sharing with e-vendors: The roles of incentives and trust," *International Journal of Electronic Commerce*, 14 (3), 63–91.

Prosser, William L (1960), "Privacy," *California Law Review*, 48 (3), 383–423.

Purcell, Kristen, Joanna Brenner, and Lee Rainie (2012), "Search Engine Use."

PwC (2014), "Consumer privacy: What are consumers willing to share?," *The speed of life: Consumer intelligence series*.

Reinartz, Werner J., Michael Haenlein, and Jörg Henseler (2009), "An empirical comparison of the efficacy of covariance-based and variance-based SEM," *International Journal of Research in Marketing*, 26 (4), 332–44.

Reinsel, David, John Gantz, and John Rydning (2017), "Data Age 2025."

Rifon, Nora J., Robert LaRose, and Sejung Marina Choi (2005), "Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures," *Journal of Consumer Affairs*, 39 (2), 339–62.

Ringle, Christian M., Sven Wende, and Jan-Michael Becker (2015), "SmartPLS 3," Bönningstedt.

Röber, Björn, Olaf Rehse, Robert Knorrek, and Benjamin Thomsen (2015), "Personal data: How context shapes consumers' data sharing with organizations from various sectors," *Electronic Markets*, 25 (2), 95–108.

Rogers, Ronald W. (1975), "A protection motivation theory of fear appeals and attitude change," *Journal of Psychology*, 91 (1), 9–114.

Rose, John, Olaf Rehse, and Björn Röber (2012), "The value of our digital identity."

Roselius, Ted (1971), "Consumer rankings of risk reduction methods," *Journal of Marketing*, 35 (1), 56–61.

Rossi, Peter E. and Greg M. Allenby (2003), "Bayesian statistics and marketing," *Marketing Science*, 23 (3), 304–28.

Rossiter, John R. (2002), "The C-OAR-SE procedure for scale development in marketing," *International Journal of Research in Marketing*, 19 (4), 305–35.

——— (2011), *Measurement for the Social Sciences*, *Springer*.

Rust, Roland T. and Ming-Hui Huang (2014), "The service revolution and the transformation of marketing science," *Marketing Science*, 33 (2), 206–21.

———, P.K. Kannan, and Na Peng (2002), "The customer economics of internet privacy," *Journal of the Academy of Marketing Science*, 30 (4), 455–64.

Schlosser, Ann E., Tiffany Barnett White, and Susan M. Lloyd (2006), "Converting web site visitors into buyers: How web site investment increases consumer trusting beliefs and online purchase intentions," *Journal of Marketing*, 70 (2), 133–48.

Schneider, Matthew J., Sharan Jagpal, Sachin Gupta, Shaobo Li, and Yan Yu (2017), "Protecting customer privacy when marketing with second-party data," *International Journal of Research in Marketing*, In Press, 1–11.

Schoenbachler, Denise D. and Geoffrey L. Gordon (2002), "Trust and customer willingness to provide information in database-driven relationship marketing," *Journal of Interactive Marketing*, 16 (3), 2–16.

Schumann, Jan H., Florian Von Wangenheim, and Nicole Groene (2014), "Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services," *Journal of Marketing*, 78 (1), 59–75.

Schwaig, Kathy S., Albert H. Segars, Varun Grover, and Kirk D. Fiedler (2013), "A model of consumers' perceptions of the invasion of information privacy," *Information & Management*, 50 (1), 1–12.

Sheehan, Kim Bartel and Mariea Grubbs Hoy (2000), "Dimensions of privacy concern among online consumers," *Journal of Public Policy & Marketing*, 19 (1), 62–73.

Shen, Anyuan and A. Dwayne Ball (2009), "Is personalization of services always a good thing? Exploring the role of technology-mediated personalization (TMP) in service relationships," *Journal of Services Marketing*, 23 (2), 79–91.

Simonson, Itamar (2005), "Determinants of customers' responses to customized offers: Conceptual framework and research propositions," *Journal of Marketing*, 69 (1), 32–45.

Slater, Stanley F. and John C. Narver (2000), "Intelligence generation and superior customer value," *Journal of the Academy of Marketing Science*, 28 (1), 120–27.

Slovic, P. (2000), "What does it mean to know a cumulative risk? Adolescents' perceptions of short-term and long-term consequences of smoking," *Journal of Behavioral Decision Making*, 13 (2), 249–66.

Smith, Jeff H., Tamara Dinev, and Heng Xu (2011), "Information privacy research: An interdisciplinairy review," *MIS Quarterly*, 35 (4), 989–1015.

———, Sandra J. Milberg, and Sandra J. Burke (1996), "Information privacy: Measuring individuals' concerns about organizational practices," *MIS Quarterly*, 20 (2), 167–96.

Smith, Jeffery S., Mark R. Gleim, Stacey G. Robinson, William J. Kettinger, and Sung-Hee Park (2014), "Using an old dog for new tricks: A regulatory focus perspective on consumer acceptance of RFID applications," *Journal of Service Research*, 17 (1), 85–101.

Solove, Daniel J. (2006), "A taxonomy of privacy," *University of Pennsylvania Law Review*, 154 (1291), 477–564.

Son, Jai-Yeol and Sung S. Kim (2008), "Internet users' information privacy-protective responses: A taxonomy and a nomological model," *MIS Quarterly*, 32 (3), 503–29.

Spärck Jones, Karen (2003), "Privacy: What's different now?," *Interdisciplinary Science Reviews*, 28 (4).

Steenkamp, Jan-Benedict E. M. and Inge Geyskens (2006), "How country characteristics affect the perceived value of web sites," *Journal of Marketing*, 70 (3), 136–50.

Stewart, David A. (2017), "A comment on privacy," *Journal of the Academy of Marketing Science*, 45 (2), 156–59.

Stone, Eugene F., Hal G. Gueutal, Donald G. Gardner, and Stephen McClure (1983), "A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations," *Journal of Applied Psychology*, 68 (3), 459–68.

Stone, Robert N. and Kjell Grønhaug (1993), "Perceived risk: Further considerations for the marketing discipline," *European Journal of Marketing*, 27 (3), 39–50.

Sutanto, Juliana, Elia Palme, Chuan-Hoo Tan, and Chee Wei Phang (2013), "Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users," *MIS Quarterly*, 37 (4), 1141–64.

Taylor, Jennifer Fries, Jodie Ferguson, and Pamela Scholder Ellen (2015), "A multi-level model of individual information privacy beliefs," *Journal of Consumer Marketing*, 32 (2), 99–112.

The Guardian (2015), "Privacy fears over 'smart' Barbie that can listen to your kids," *[Accessed on: 28-08-2017]*.

TNS (2011), "Attitudes on data protection and electronic identity in the European Union."

Tourangeau, Roger and Ting Yan (2007), "Sensitive questions in surveys," *Psychological bulletin*, 133 (5), 859–83.

TRUSTe (2016), "U.S. Consumer Privacy Index."

Tsai, Janice Y., Serge Egelman, Lorrie Faith Cranor, and Alessandro Acquisti (2011), "The effect of online privacy information on purchasing behavior: An experimental study," *Information Systems Research*, 22 (2), 254–68.

Tucker, Catherine E. (2014), "Social networks, personalized advertising, and privacy controls," *Journal of Marketing Research*, 51 (5), 546–62.

Turow, Joseph, Jennifer King, Chris Jay Hoofnagle, Amy Bleakley, and Michael Hennessy (2009), "Americans reject tailored advertising and three activities that enable it," *Working Paper*.

Tversky, Amos and Daniel Kahneman (1981), "The framing of decisions and the psychology of choice," *Science*, 211 (4481), 453–58.

Urban, Glen L., Guilherme (Gui) Liberali, Erin MacDonald, Robert Bordley, and John R. Hauser (2013), "Morphing banner advertising," *Marketing Science*, 33 (1), 27–46.

Urban, Jennifer M. and Chris Jay Hoofnagle (2014), "The privacy pragmatic as privacy vulnerable," in *Symposium on Usable Privacy and Security (SOUPS)*.

Verhoef, Peter C., Edwin Kooge, and Natasha Walk (2016), *Creating value with big data analytics: Making smarter marketing decisions*, Routledge.

Vroom, V. H. (1964), *Work and motivation*, New York, New York, USA: Wiley.

Wang, Sijun, Sharon E. Beatty, and William Foxx (2004), "Signaling the trustworthiness of small online retailers," *Journal of Interactive Marketing*, 18 (1), 53–69.

Warren, Samuel D. and Louis D. Brandeis (1890), "The right to privacy," *Harvard Law Review*, 4 (5), 193–220.

Wedel, Michel and P.K. Kannan (2016), "Marketing analytics for data-rich environments," *Journal of Marketing*, 80 (6), 97–121.

Westin, Alan F. (1967), *Privacy and freedom*, New York, New York, USA: Atheneum.

White, Tiffany Barnett (2004), "Consumer disclosure and disclosure avoidance: A motivational framework," *Journal of Consumer Psychology*, 14 (1–2), 41–51.

———, Thomas P. Novak, and Donna L. Hoffman (2014), "No strings attached: When giving it away versus making them pay reduces consumer information disclosure," *Journal of Interactive Marketing*, 28 (3), 184–95.

———, Debra L. Zahay, Helge Thorbjørnsen, and Sharon Shavitt (2008), "Getting too personal: Reactance to highly personalized email solicitations," *Marketing Letters*, 19 (1), 39–50.

Wirtz, Jochen and May O. Lwin (2009), "Regulatory focus theory, trust, and privacy concern," *Journal of Service Research*, 12 (2), 190–207.

Wlömert, Nils and Felix Eggers (2016), "Predicting new service adoption with conjoint analysis: External validity of BDM-based incentive aligned and dual-response choice designs," *Marketing Letters*, 27 (1), 195–210.

Wolfinbarger, Mary and Mary C. Gilly (2003), "eTailQ: Dimensionalizing, measuring and predicting etail quality," *Journal of Retailing*, 79 (3), 183–98.

World Economic Forum (2014a), "Rethinking personal data: Trust and context in user-centred data ecosystems."

——— (2014b), “Rethinking personal data: A new lens for strengthening trust.”

Xie, En, Hock-Hai Teo, and Wen Wan (2006), “Volunteering personal information on the internet: Effects of reputation, privacy notices, and rewards on online consumer behavior,” *Marketing Letters*, 17 (1), 61–74.

Xie, Jierui, Bart P. Knijnenburg, and Hongxia Jin (2014), “Location sharing privacy preference,” in *IUI*, 189–98.

Xu, Heng, Robert E. Crossler, and France Bélanger (2012), “A value sensitive design Investigation of privacy enhancing tools in web browsers,” *Decision Support Systems*, 54 (1), 424–33.

———, Xin (Robert) Luo, John M. Carroll, and Mary Beth Rosson (2011), “The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing,” *Decision Support Systems*, 51 (1), 42–52.

———, Hock-Hai Teo, Bernard C.Y. Tan, and Ritu Agarwal (2009), “The role of push-pull technology in privacy calculus: The case of location-based services,” *Journal of Management Information Systems*, 26 (3), 135–73.

———, ———, ———, and ——— (2012), “Research Note - Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services,” *Information Systems Research*, 23 (4), 1342–63.

Youn, Seounmi (2009), “Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents,” *Journal of Consumer Affairs*, 43 (3), 389–419.

Zaichkowsky, Judith Lynne (1985), “Measuring the involvement construct,” *Journal of*

*Consumer Research*, 12 (3), 341–52.

Zhang, Jie and Michel Wedel (2009), "The effectiveness of customized promotions in online and offline stores," *Journal of Marketing Research*, 46 (4), 190–206.

Zhao, Ling, Yaobin Lu, and Sumeet Gupta (2012), "Disclosure intention of location-related information in location-based social network services," *International Journal of Electronic Commerce*, 16 (4), 53–89.

Zimmer, J. Christopher, Riza Arsal, Mohammad Al-Marzouq, Dewayne Moore, and Varun Grover (2010), "Knowing your customers: Using a reciprocal relationship to enhance voluntary information disclosure," *Decision Support Systems*, 48 (2), 395–406.

# Chapter 7.

# Appendices

**Appendix A.** Item purification (Financial) – Chapter 3 (STUDY 1)

| Item | Valence | | Probability | | VIF | | Weight | | Loading | | Reformulation / Reason for removal |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | μ | σ | μ | σ | Before | After | Before | After | Before | After | |
| I receive monetary compensation | 1.91 | 1.21 | 4.03 | 1.93 | 1.571 | 1.534 | -0.081 | -0.059 | 0.266 | 0.308 | I receive monetary compensation |
| I have access to monetary savings (i.e., discounts) | 2.02 | 0.99 | 5.15 | 1.43 | 2.396 | 1.787 | -0.056 | 0.145 | 0.416 | 0.459 | I have access to monetary savings (i.e., discounts) |
| *[Your Firm]* is able to provide its customers with low prices (e.g., due to more efficient business operations) | 1.76 | 1.11 | 4.29 | 1.61 | 2.598 | 1.705 | 0.059 | 0.187 | 0.449 | 0.496 | *[Your Firm]* is able to provide its customers with low prices in general (e.g., due to more efficiency, customer insights) |
| *[Your Firm]* adapts it's prices to my personal profile | 0.64 | 1.49 | 3.99 | 1.56 | 1.387 | 1.321 | 0.338 | 0.434 | 0.694 | 0.738 | *[Your Firm]* adapts it's prices to my personal profile |
| I receive discounts that fit my personal needs or preferences | 1.82 | 1.07 | 4.81 | 1.42 | 2.345 | N/A | 0.346 | N/A | 0.583 | N/A | REMOVED – *Round 1 (duplicate)* |
| *[Your Firm]* charges me lower prices than other customers for similar products or services | 1.92 | 1.13 | 3.98 | 1.51 | 2.491 | N/A | 0.043 | N/A | 0.374 | N/A | REMOVED – *Round 1 (duplicate)* |
| *[Your Firm]* is able to generate additional money using my personal information | -1.02 | 1.59 | 4.94 | 1.74 | 1.173 | 1.169 | 0.446 | 0.428 | 0.703 | 0.701 | *[Your Firm]* is able to generate additional revenues |
| *[Your Firm]* charges additional money from my credit or bankcard | -2.67 | 0.75 | 3.04 | 1.83 | 1.852 | 1.147 | 0.309 | 0.387 | 0.607 | 0.618 | *[Your Firm]* charges additional money from my credit card or bankcard |
| I pay higher prices than other customers for the same products or services | -2.53 | 0.78 | 2.67 | 1.62 | 1.762 | NA | 0.123 | N/A | 0.526 | N/A | REMOVED – *Round 1 (duplicate)* |

**Appendix A.** Item purification (Performance) – Chapter 3 (STUDY 1)

| Item | Valence | | Probability | | VIF | | Weight | | Loading | | Reformulation / Reason for removal |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | μ | σ | μ | σ | Before | After | Before | After | Before | After | |
| Products and/or services are adapted to my personal preferences | 1.08 | 1.26 | 5.07 | 1.38 | 2.434 | 1.663 | 0.235 | 0.330 | 0.727 | 0.765 | Products and/or services of *[Your Firm]* are adapted to my personal preferences |
| I am denied certain services or products | -2.22 | 0.92 | 2.88 | 1.62 | 1.090 | 1.042 | 0.427 | 0.447 | 0.507 | 0.498 | I am denied certain services and/or products |
| *[Your Firm]* predicts my future needs and preferences | 0.57 | 1.35 | 4.52 | 1.53 | 2.231 | N/A | 0.214 | N/A | 0.733 | N/A | REMOVED – *Round 1 (duplicate)* |
| Their communication is tailored to my personal preferences | 1.25 | 1.12 | 4.76 | 1.30 | 3.579 | N/A | 0.031 | N/A | 0.686 | N/A | REMOVED – *Round 1 (too generic)* |
| They are less likely to make errors when I interact or transact with them | 1.60 | 1.30 | 3.80 | 1.48 | 1.924 | 1.563 | 0.033 | 0.094 | 0.495 | 0.532 | *[Your Firm]* makes fewer errors when I interact or transact with them |
| *[Your Firm]* knows my personal needs or preferences | 0.50 | 1.42 | 4.70 | 1.40 | 2.296 | N/A | 0.247 | N/A | 0.760 | N/A | REMOVED – *Round 2 (duplicate)* |
| *[Your Firm]* gives recommendations based on my personal needs and preferences | 1.05 | 1.25 | 4.96 | 1.46 | 3.379 | N/A | -0.026 | N/A | 0.682 | N/A | REMOVED – *Round 1 (duplicate)* |
| I am able to use products or services without limitations or constraints | 1.65 | 1.22 | 4.08 | 1.55 | 2.555 | N/A | 0.111 | N/A | 0.523 | N/A | REMOVED – *Round 1 (duplicate)* |
| *[Your Firm]* is more attentive in their services to me | 1.38 | 1.25 | 4.13 | 1.52 | 3.090 | N/A | -0.090 | N/A | 0.617 | N/A | REMOVED – *Round 1 (too generic)* |
| *[Your Firm]* provides a personalized experience | 1.27 | 1.14 | 4.93 | 1.41 | 3.235 | N/A | -0.090 | N/A | 0.579 | N/A | REMOVED – *Round 1 (too generic)* |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Employees of *[Your Firm]* provide me with personalized responses | 1.24 | 1.17 | 4.31 | 1.55 | 2.557 | N/A | 0.112 | N/A | 0.662 | N/A | REMOVED – *Round 2 (duplicate / low importance)* |
| I receive better service than other customers | 1.71 | 1.20 | 3.86 | 1.49 | 2.077 | 1.882 | 0.002 | 0.108 | 0.543 | 0.596 | I receive better service than other customers |
| I receive feedback which allows me to make better decisions | 1.15 | 1.20 | 4.21 | 1.51 | 2.301 | 1.920 | 0.273 | 0.387 | 0.713 | 0.764 | I receive information or feedback giving insights in my own behavior or decisions |
| I have access to free (additional) services or content | 1.87 | 1.10 | 4.52 | 1.44 | 2.391 | 1.870 | 0.003 | 0.046 | 0.515 | 0.555 | I have access to free (additional) services or content |
| *[Your Firm]* filters which information in their communication (e.g., advertisements) is relevant for me | 0.73 | 1.42 | 4.68 | 1.40 | 1.867 | 1.576 | 0.054 | 0.140 | 0.591 | 0.634 | I receive communication (e.g., advertisements) that is tailored to my personal needs or preferences |
| I receive information that fits my current needs or situation | 1.29 | 1.11 | 4.71 | 1.45 | 2.940 | N/A | -0.012 | N/A | 0.599 | N/A | REMOVED – *Round 2 (duplicate / low importance)* |

**Appendix A.** Item purification (Psychological) – Chapter 3 (STUDY 1)

| Item | Valence | | Probability | | VIF | | Weight | | Loading | | Reformulation / Reason for removal |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | μ | σ | μ | σ | Before | After | Before | After | Before | After | |
| It feels like *[Your Firm]* knows a lot about me | -0.96 | 1.41 | 4.96 | 1.47 | 2.185 | 1.918 | 0.203 | 0.247 | 0.785 | 0.794 | It feels like *[Your Firm]* knows a lot about me |
| It feels like *[Your Firm]* follows my everyday behavior | -1.85 | 1.27 | 4.79 | 1.69 | 3.276 | 1.789 | 0.097 | 0.327 | 0.717 | 0.743 | It feels like *[Your Firm]* follows my behavior |
| It feels like *[Your Firm]* is constantly monitoring me | -2.20 | 0.99 | 4.63 | 1.80 | 2.986 | N/A | 0.221 | N/A | 0.701 | N/A | REMOVED – *Round 1 (duplicate)* |
| It feels like *[Your Firm]* enters my personal life | -1.83 | 1.21 | 4.54 | 1.71 | 3.446 | N/A | -0.002 | N/A | 0.710 | N/A | REMOVED – *Round 1 (duplicate)* |
| It feels like *[Your Firm]* controls the collection, storage, and use of my personal information | -1.50 | 1.46 | 4.76 | 1.64 | 2.055 | 1.837 | 0.157 | 0.250 | 0.712 | 0.738 | It feels like *[Your Firm]* controls the collection, storage, and use of my personal information |
| It feels like I have less freedom of choice | -1.77 | 1.29 | 3.46 | 1.73 | 1.501 | N/A | 0.215 | N/A | 0.575 | N/A | REMOVED – *Round 2 (low importance)* |
| I have a closer relationship with *[Your Firm]* | 0.59 | 1.28 | 3.61 | 1.56 | 1.892 | 1.854 | 0.145 | 0.147 | 0.641 | 0.669 | My relationship with *[Your Firm]* becomes closer |
| *[Your Firm]* makes me feel special | 1.35 | 1.24 | 3.52 | 1.71 | 1.918 | 1.916 | 0.236 | 0.227 | 0.655 | 0.670 | *[Your Firm]* makes me feel special |
| I have the possibility to express myself | 0.97 | 1.17 | 3.64 | 1.62 | 1.678 | 1.669 | 0.225 | 0.208 | 0.595 | 0.603 | I have the possibility to express myself |

**Appendix A.** Item purification (Time) – Chapter 3 (STUDY 1)

| Item | Valence | | Probability | | VIF | | Weight | | Loading | | Reformulation / Reason for removal |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | μ | σ | μ | σ | Before | After | Before | After | Before | After | |
| I can find the right product or service faster | 1.91 | 1.01 | 4.70 | 1.48 | 2.194 | 1.317 | 0.400 | 0.497 | 0.633 | 0.653 | I can find the right product or service faster |
| The process of completing transactions is (partly) automated | 0.92 | 1.76 | 4.78 | 1.34 | 1.403 | 1.347 | 0.116 | 0.141 | 0.508 | 0.513 | The process of completing transactions is (partly) automated |
| Interactions with *[Your Firm]* are more efficient | 1.84 | 1.04 | 4.55 | 1.60 | 2.174 | N/A | 0.135 | N/A | 0.549 | N/A | REMOVED – Round 1 *(duplicate)* |
| I have to provide the same information multiple times | -1.29 | 1.26 | 3.89 | 1.61 | 1.271 | N/A | 0.203 | N/A | 0.524 | N/A | REMOVED – Round 2 (*less important*) |
| I have to provide *[Your Firm]* with additional (personal) information | -1.55 | 1.33 | 4.75 | 1.64 | 1.307 | 1.619 | 0.631 | 0.583 | 0.804 | 0.796 | I have to fill in forms to provide *[Your Firm]* with additional (personal) information |
| I have to actively protect my (online) identity | -0.94 | 1.84 | 4.90 | 1.67 | 1.343 | 1.241 | 0.140 | 0.122 | 0.530 | 0.481 | I have to take the time to protect my (online) identity |
| I need to monitor how *[Your Firm]* stores and uses my information | -1.36 | 1.52 | 4.98 | 1.64 | 1.702 | 1.406 | 0.092 | 0.148 | 0.585 | 0.537 | I have to take the time to monitor how *[Your Firm]* handles my information |
| I have to monitor whether the databases of *[Your Firm]* contain any errors | -1.75 | 1.19 | 3.66 | 1.65 | 1.894 | N/A | -0.042 | N/A | 0.572 | N/A | REMOVED – *Round 2* |

**Appendix A.** Item purification (Social) – Chapter 3 (STUDY 1)

| Item | Valence | | Probability | | VIF | | Weight | | Loading | | Reformulation / Reason for removal |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | μ | σ | μ | σ | Before | After | Before | After | Before | After | |
| I have the possibility to connect with friends and family | 0.76 | 1.35 | 3.85 | 1.51 | 1.179 | 1.179 | 0.410 | 0.425 | 0.641 | 0.659 | I can connect with friends and family |
| I have to explain to my family and friends why I shared personal information | -1.64 | 1.21 | 3.08 | 1.63 | 1.289 | 1.289 | 0.246 | 0.202 | 0.571 | 0.535 | I have to explain to my family and friends why I shared personal information |
| My family and friends receive all kinds of communication (e.g. advertisements) that is adapted to my personal needs | -1.69 | 1.45 | 3.75 | 1.77 | 1.304 | 1.304 | 0.405 | 0.412 | 0.720 | 0.715 | My family and friends receive communication (e.g., advertisements) that is adapted to my personal needs |
| Family and friends know exactly in which products and services I am interested | -0.67 | 1.52 | 3.64 | 1.47 | 1.382 | 1.382 | 0.393 | 0.406 | 0.776 | 0.782 | Family and friends become aware which product or services I am interested in |

**Appendix A.** Item purification (Security) – Chapter 3 (STUDY 1)

| Item | Valence | | Probability | | VIF | | Weight | | Loading | | Reformulation / Reason for removal |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | μ | σ | μ | σ | Before | After | Before | After | Before | After | |
| My personal information is stored in an unsafe location | -2.46 | 0.97 | 3.86 | 1.75 | 3.489 | N/A | -0.117 | N/A | 0.718 | N/A | REMOVED – *Round 1 (too generic)* |
| My personal information ends up with other companies | -2.35 | 0.95 | 4.57 | 1.85 | 4.043 | 2.918 | -0.067 | 0.187 | 0.760 | 0.837 | My personal information ends up with other firms or organizations |
| My personal information ends up with unknown. third parties if *[Your Firm]* goes bankrupt | -2.61 | 0.87 | 4.00 | 2.06 | 3.329 | N/A | 0.023 | N/A | 0.751 | N/A | REMOVED – *Round 1 (duplicate)* |
| My personal information ends up with governmental institutions | -1.97 | 1.20 | 4.28 | 1.89 | 1.973 | N/A | 0.180 | N/A | 0.712 | N/A | REMOVED – *Round 2 (low importance)* |
| My online identity will be stolen | -2.74 | 0.72 | 3.47 | 1.68 | 4.748 | N/A | 0.019 | N/A | 0.716 | N/A | REMOVED – *Round 1 (duplicate)* |
| My personal information will be used for (identity) fraud | -2.56 | 1.13 | 3.44 | 1.75 | 2.100 | 1.740 | 0.042 | 0.109 | 0.601 | 0.655 | My personal information will be used for (identity) fraud |
| Unknown outsiders will intercept my personal information | -2.63 | 0.80 | 3.61 | 1.71 | 6.333 | N/A | 0.185 | N/A | 0.788 | N/A | REMOVED – *Round 1 (duplicate)* |
| My personal information will become accidently publicly available | -2.60 | 0.81 | 3.56 | 1.68 | 4.795 | 2.677 | 0.212 | 0.335 | 0.792 | 0.872 | My personal information will become (accidently) publicly available |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| The security of my personal information depends on the stability of information systems | -1.41 | 1.42 | 5.13 | 1.50 | 2.314 | 1.920 | 0.173 | 0.335 | 0.749 | 0.835 | It depends on the stability of information systems whether my information is kept safe |
| *[Your Firm]* sends me (unrequested) communication | -1.75 | 1.16 | 4.87 | 1.78 | 2.160 | N/A | 0.447 | N/A | 0.807 | N/A | REMOVED – *Round 2 (duplicate)* |
| Personal information about me will be made public | -2.45 | 0.97 | 4.08 | 1.89 | 2.727 | N/A | 0.083 | N/A | 0.746 | N/A | REMOVED – *Round 1 (duplicate)* |
| My personal information is visible for others, like employees | -2.03 | 1.24 | 4.49 | 1.78 | 2.841 | 2.540 | 0.019 | 0.167 | 0.743 | 0.817 | My personal information is visible for other people, like employees |
| I receive (unrequested) communication from companies other than *[Your Firm]* | -2.14 | 1.08 | 5.00 | 1.88 | 2.239 | 1.730 | -0.100 | 0.095 | 0.618 | 0.673 | I receive (unrequested) communication |
| It feels like *[Your Firm]* can always use my personal information later on for secondary purposes | -2.18 | 1.07 | 4.68 | 1.79 | 3.587 | N/A | 0.042 | N/A | 0.766 | N/A | REMOVED – Round 2 |
| I feel vulnerable for security risks | -2.47 | 0.91 | 4.43 | 1.82 | 3.567 | N/A | -0.006 | N/A | 0.718 | N/A | REMOVED – *Round 1 (duplicate)* |

**Appendix B.** Scenarios – Chapter 3 (STUDY 1)

**Scenario 1: Online retailer**

*[Your Firm]* recently introduced a new savings program, in which consumers can not only accumulate points based on their purchases, but also on the extent to which consumers share their purchases with their social environment via all kinds of social media. Consumers can use these points for various discounts, additional service, or even free products.

In order to provide this service, *[Your Firm]* needs your permission to record your purchases at an individual level, record whether you share your purchases with others, and link them to your personal profile.

**Scenario 2: Telecom operator**

*[Your Firm]* plans on introducing a new service, which provides relevant personalized offers and information to their customers, based on customer's physical location. As a result, you will receive discounts (coupons), which you can immediately redeem considering they relate to your actual physical location.

However, for this service *[Your Firm]* needs your permission to record your exact location, and combine this with information derived from different sources, ranging from the browsing behavior on your mobile phone to information derived from external sources.

**Scenario 3: Bank**

*[Your Firm]* plans on introducing a new service, which not only allows you to better monitor your spending behavior, but also allows *[Your Firm]* providing you with personalized offerings. As a result, you will receive discounts (coupons) via e-mail from a number of firms based on your needs and preferences.

However, for this service *[Your Firm]* needs your permission to use the exact time and location (store) of all your spendings to create your personalized spending overview. In addition, they need permission to share your spending behavior linked to your customer ID with other firms, so they can provide offerings that fit your actual needs and preferences.

## **Appendix C.** Scenarios – Chapter 3 (STUDY 2) (*translated*)

**Scenario 1: Telecom operator**

*[Your Firm]* plans on introducing a new service, which provides personalized offers and information to consumers based on their physical location. This means that you as a consumer will receive personalized discounts (coupons) based on your physical location, useful information regarding your environment, and other relevant offerings linked to your actual physical location.

However, for this service *[Your Firm]* needs your permission to record your location, and combine this with information derived from other sources. For example, *[Your Firm]* wants to connect your location to your browsing information, and other information acquired from third parties. Next to providing you with this personalized service *[Your Firm]* aims to use the information for aggregated, internal analyses. These analyses will also benefit their customers as it provides them a better insight in the needs and preferences of consumers.

**Scenario 2: Insurance**

In order to better serve their customers, *[Your Firm]* recently introduced a new type of car insurance. By recording your driving behavior *[Your Firm]* is able to provide their customers insights regarding their driving behavior, and how to drive more safely. Moreover, *[Your Firm]* adapts the costs of their car insurance based on your actual driving behavior, giving you a reward when you drive more safely than the average driver.

In order to provide this service, *[Your Firm]* needs permission to record where you drive, when you drive, and how you drive using an easy-to-install chip in your car. *[Your Firm]* uses this information to provide you insights, give you tips, and adapt your insurance premium. In addition, *[Your Firm]* aims to use the information for aggregated, internal analyses. These analyses will also benefit their customers as it provides them a better insight in the needs and preferences of consumers. How likely is it that you would accept this new car insurance, and grant *[Your Firm]* permission to record your driving behavior?

**Appendix D.** Measurement items for the other constructs[9]

**Willingness to accept** (self-developed, Chapter 3 – Study 1 and 2)

1. How likely is it that you would accept this service? (1: Very unlikely … 7: Very likely)

**Behavioral loyalty** (self-developed, Chapter 3 – Study 2, Chapter 4)

1. How many years are you already a customer of *[Your Firm]*? *(Less than a week – More than a week, less than a month – More than a month, less than three months – More than three months, less than a year – More than a year, less than two years – More than two years, less than five years – More than five years)*

**Specific trust beliefs** (McKnight, Choudhury, and Kacmar 2002) (Chapter 3 – Study 2: $\alpha = 0.953$)

Benevolence ($\alpha = 0.846$)

1. I believe *[Your Firm]* would act in my best interest
2. If I required help, *[Your Firm]* would do its best to help me
3. *[Your Firm]* is interested in my well-being, not just its own

Integrity ($\alpha = 0.915$)

4. *[Your Firm]* is truthful in its dealing with me
5. I would characterize *[Your Firm]* as honest
6. *[Your Firm]* would keep its commitments
7. *[Your Firm]* is sincere and genuine

Competence ($\alpha = 0.945$)

8. *[Your Firm]* is competent and effective in her service
9. *[Your Firm]* performs its role as producer / service provider very well
10. *[Your Firm]* is capable and proficient

[9] All items are measured using 7-point Likert scales (strongly disagree … strongly agree), unless stated otherwise.

11. In general, *[Your Firm]* is very knowledgeable about this specific type of product or service

**Concern for information privacy** (Smith, Milberg, and Burke 1996) (Chapter 3 – Study 2: α = 0.909)

Collection (α = 0.824)

1. It bothers me when *[Your Firm]* asks me for my personal information
2. When *[Your Firm]* asks me for personal information, I sometimes think twice before providing it
3. It bothers me to give so much personal information to *[Your Firm]*
4. I'm concerned that *[Your Firm]* is collecting too much personal information about me

Errors (α = 0.899)

5. *[Your Firm]* has to double-check the accuracy of all personal information in computer database —no matter how much this costs.
6. *[Your Firm]* should take more steps to make sure that the personal information in their files is accurate.
7. *[Your Firm]* should have better procedures to prevent and correct errors in personal information.
8. *[Your Firm]* should devote a lot of time and effort in verifying the accuracy of the personal information in their databases.

Unauthorized access (α = 0.814)

9. *[Your Firm]* should devote more effort in preventing unauthorized access to personal information
10. *[Your Firm]* should protect the databases that contain personal information from unauthorized access, no matter how much it costs

11. *[Your Firm]* should take more steps to make sure that unauthorized people cannot access personal information in their computers

Secondary use (α = 0.894)

12. *[Your Firm]* should not use personal information for any purpose unless it has been authorized by the individuals who provided the information
13. When individuals give personal information to *[Your Firm]* for some reason, *[Your Firm]* should never use the information for any other reason.
14. *[Your Firm]* should never sell the personal information in their computer databases to other companies.
15. *[Your Firm]* should never share personal information with other unless it has been authorized by the individuals who provided the information

**Personality** (Gosling, Rentfrow, and Swann 2003) (Chapter 3 – Study 2)

Agreeableness (ρ = -0.325)

1. I see myself as sympathetic
2. I see myself as critical (R)*

Conscientiousness (ρ = 0.369)

3. I see myself as dependable/self-disciplined
4. I see myself as disorganized/careless (R)*

Emotional instability (ρ = 0.394)

5. I see myself as calm/emotionally stable (R)*
6. I see myself as anxious/easily upset

Extraversion (ρ = -0.057)

7. I see myself as extraverted/enthusiastic*
8. I see myself as reserved/quiet (R)

Openness to new experience (ρ = 0.208)

9. I see myself as open to new experiences/complex*
10. I see myself as conventional/uncreative (R)

** These items represented the construct the best and were used for further analyses*

**Privacy violation experience** (Direct and Indirect) (Xu et al. 2011) (Chapter 3 – Study 2 and 3)

1. How often during the past year have you personally been victim of what you felt was an invasion of privacy? *(Never – Once – 2 to 5 times – 6 to 10 times – More than 10 times)*
2. How much have you heard or read during the last year about what you felt was an invasion of privacy? *(Never – Once – 2 to 5 times – 6 to 10 times – More than 10 times)*

**Privacy protective behavior** (self-developed, Chapter 3 – Study 2)

1. Have you ever changed the standard cookie settings of your web browser (e.g. Internet Explorer, Google Chrome, Mozilla Firefox, Safari)? *(Yes – No)*
2. Have you ever changed the standard privacy settings of your social media accounts (e.g. Facebook, Twitter, Instagram)? *(Yes – No)*
3. Do you make use of an (online) ad blocker? *(Yes – No)*
4. How often do you read the privacy statement on a website? *(Never – Once in a while – Almost always – Always – N/A)*
5. How often have you refused to install an app on your mobile phone because of too many information collection requests? *(Never – Once in a while – Almost always – Always – N/A)*
6. How often do you purposely provide errant information online (e.g. email, name)? *(Never – Once in a while – Almost always – Always – N/A)*

**General trust beliefs** (Morgan and Hunt 1994) (Chapter 3 – Study 2: α = 0.910, Study 3: α = 0.947, Chapter 4: α = 0.960)

1. I trust *[Your Firm]* completely
2. *[Your Firm]* can be counted on to do what is right
3. One can rely on *[Your Firm]*

**General privacy concern** (Dinev and Hart 2006) (Chapter 3 – Study 2: $\alpha = 0.915$, Study 3: $\alpha = 0.946$)

1. I am concerned that the information I submit on the Internet could be misused
2. I am concerned that a person can find private information about me on the Internet
3. I am concerned about submitting information on the Internet, because of what others might do with it
4. I am concerned about submitting information on the Internet, because it could be used in a way I did not foresee.

**Information sensitivity** (self-developed, Chapter 3 – Study 2)

1. How sensitive would you consider the information *[Your Firm]* wants to collect about you? *(1. Totally not sensitive … 7. Very sensitive)*

**Involvement** (Mittal 1989) (Chapter 3 – Study 2: $\alpha = 0.893$, Study 3: $\alpha = 0.858$)

1. I am very deliberate in [acceptance of mobile services/usage of social media/taking out a car insurance]
2. Which [mobile service I accept/social media I use/car insurance I take out] is important for me
3. The choice for a [mobile service/social media/car insurance] is an important decision for me

**Innovativeness** (Xu et al. 2011) (Chapter 3 – Study 3: $\alpha = 0.927$)

1. If I hear about a new technology, I would look for ways to try out the technology
2. In my social environment, I am usually the first to try out new technologies

3. I like to try out new technologies immediately

**Customer satisfaction** (Chapter 4)

1. How satisfied are you with the products and/or services offered by *[Your Firm]*? (1: Not satisfied … 7: Satisfied)

**Industry characteristics** (Chapter 4)

1. *Interaction intensity* – How often do you make use of the products and/or services offered by *[Your Firm]?* (1: Daily … 7: Less than once a year)
2. *Information sensitivity* – How sensitive do you consider the information *[Your Firm]* collects? (1: Not sensitive … 7: Sensitive)
3. *Involvement* – The products and/or services of *[Your Firm]* are very important for me.
4. *Competitive intensity* – There are many alternative providers for the products and/or services of *[Your Firm]*.
5. *Privacy concern (industry)* – I am very worried about the privacy of *[Your Firm]*
6. *Personalization value* – It would be really valuable if the products and/or services of *[Your Firm]* would be tailored to my personal needs
7. *Governmental regulation* – *[Your Firm]* has to deal with much privacy legislation
8. *Utilitarian* – I obtain the products and/or services of *[Your Firm]* because they are very useful to me
9. *Hedonic* – I obtain the products and/or services of *[Your Firm]* because they are fun

**General privacy concern** (Lwin et al. 2016) (Chapter 4: $\alpha = 0.82$)

1. When firms ask me for personal information, I would think twice before providing it
2. It usually bothers me when firms ask me for personal information.
3. I am concerned about providing information to firms

**Privacy protective behavior** (self-developed, Chapter 4)

1. Read privacy statements (1: Never … 7: Often)
2. Requested a firm to remove personal information (1: Never … 7: Often)
3. Requested to see which personal information a firm had stored (1: Never … 7: Often)
4. Refused to install an app on your mobile phone because of too many information collection requests (1: Never … 7: Often)
5. Have you ever changed the standard privacy settings of your social media accounts (e.g. Facebook, Twitter, LinkedIN)? (Yes – No)
6. Do you have installed an (online) ad or cookie blocker (e.g., AdBlock Plus, Ghostery) on your desktop or phone? (Yes – No)

**Appendix E.** Industry characteristics – Chapter 4 (pre-test, N = 50)

| Industry | Information sensitivity | Interaction intensity | Involvement | Privacy concern | Reason to buy | Personalization value | Privacy regulation | Competition |
|---|---|---|---|---|---|---|---|---|
| Electricity provider | 2.84 | 3.52 | 3.68 | 3.34 | 2.24 | 1.08 | 2.76 | 3.52 |
| Online video streaming service | 2.64 | 4.20 | 4.90 | 2.94 | 2.58 | 4.64 | 3.38 | 1.94 |
| Pharmacy | 4.40 | 3.12 | 3.36 | 3.68 | 3.46 | 1.06 | 3.88 | 4.40 |
| Dating service | 3.80 | 1.50 | 3.78 | 2.36 | 2.94 | 4.00 | 3.48 | 1.46 |
| Casino | 2.38 | 1.44 | 2.47 | 1.46 | 1.96 | 4.76 | 1.80 | 2.52 |
| Clothing retailer | 1.98 | 3.18 | 3.32 | 2.72 | 1.84 | 2.66 | 3.22 | 1.78 |
| Fitness tracker | 2.68 | 2.96 | 4.92 | 2.66 | 2.46 | 2.52 | 3.82 | 1.46 |
| Cinema | 1.90 | 2.68 | 3.05 | 1.78 | 1.52 | 4.78 | 2.30 | 1.58 |
| Bank | 4.74 | 4.84 | 4.92 | 4.54 | 4.60 | 1.10 | 4.00 | 4.68 |
| Health insurance | 4.70 | 2.78 | 3.28 | 4.64 | 4.28 | 1.12 | 4.64 | 4.64 |
| Online news provider | 1.88 | 4.30 | 5.13 | 2.64 | 2.10 | 2.44 | 2.64 | 1.70 |
| Grocery retailer | 2.20 | 4.80 | 4.88 | 3.26 | 2.04 | 1.64 | 3.18 | 2.22 |
| Electricity provider | 2.84 | 3.52 | 3.68 | 3.34 | 2.24 | 1.08 | 2.76 | 3.52 |
| ***Average*** | ***3.01*** | ***3.28*** | ***3.97*** | ***3.00*** | ***2.67*** | ***2.65*** | ***3.26*** | ***2.66*** |

**Appendix F.** Scenario description – Chapter 4 (*translated*)

Now *[Your Firm]* is thinking about introducing a new personalization program called "PLUS". This program is free of charge and aims to augment the current service of *[Your Firm]*.

At this moment *[Your Firm]* uses information about it's customers only to improve their products and services at a general level. By introducing the personalization program "PLUS" *[Your Firm]* aims to adapt it's products and services to the needs of individual customers. Therefore "PLUS" ensures that the products and services of *[Your Firm]* better fit you. Although most decisions with regard to "PLUS" have already been made there is still uncertainty about some of the terms and conditions.

On the following pages you are repeatedly asked to choose between two alternatives of "PLUS". These alternatives differ on the terms and conditions that have been mentioned before. Please select the alternative that you prefer. After this decision you are asked whether you would truly adopt the new personalization program "PLUS" and the corresponding terms and conditions. When choosing between both alternatives please assume all other characteristics of the personalization program "PLUS" are the same. In other words, both alternatives are identical except for the terms and conditions mentioned here.

**Appendix G.** List of attributes and levels (*translated*)

| |
|---|
| **Information collection**<br>1 – Volunteered information (forms)<br>2 – Volunteered + Internally collected information (click-stream)<br>3 – Volunteered + Externally collected information (search behavior)<br>4 – Volunteered + Inferred information (needs based on click-stream)<br>5 – Volunteered + Internally + Externally<br>6 – Volunteered + Internally + Inferred<br>7 – Volunteered + Internally + Externally + Inferred |
| **Information storage (type) and information storage (time)**<br>1 – Anonymous + Unlimited<br>2 – Anonymous + One year<br>3 – Anonymous + One month<br>4 – Identifiable on ID + Unlimited<br>5 – Identifiable on ID + One year<br>6 – Identifiable on ID + One month<br>7 – Identifiable on email address + Unlimited<br>8 – Identifiable on email address + One year<br>9 – Identifiable on email address + One month |
| **Information use**<br>1 – Insights in own behavior (recommendations)<br>2 – Personalized marketing content<br>3 – Dissemination with third parties<br>4 – Insights + Personalized marketing<br>5 – Insights + Dissemination with third parties<br>6 – Insights + Personalized marketing + Dissemination<br>7 – Personalized marketing + Dissemination |
| **Transparency**<br>1 – None<br>2 – Insight in collection<br>3 – Insight in storage<br>4 – Insight in use<br>5 – Insight in collection and storage<br>6 – Insight in collection and use<br>7 – Insight in collection and storage and use<br>8 – Insight in storage and use |
| **Control**<br>1 – None<br>2 – Control over collection<br>3 – Control over storage<br>4 – Control over use<br>5 – Control over collection and storage<br>6 – Control over collection and use<br>7 – Control over collection and storage and use<br>8 – Control over storage and use |

## Chapter 8.

# Nederlandse Samenvatting

In dit proefschrift bestuderen we de invloed van privacy voor bedrijven en consumenten. In ons huidige '*informatietijdperk'* is het verzamelen van informatie cruciaal geworden voor bedrijven. Echter heeft de groeiende hoeveelheid informatie consumenten ook bezorgd gemaakt over hun privacy. In de VS geeft 92% van de consumenten aan zorgen te hebben over hun online privacy (TRUSTe 2016), terwijl wereldwijd 57% van de consumenten meer bezorgd zijn over hun privacy dan vorig jaar (CIGI-Ipsos 2017). Deze zorgen een bedreiging voor bedrijven die onzorgvuldig omgaan met privacy. Naast dat consumenten tegenwoordig eenvoudiger minder informatie kunnen delen zorgt onzorgvuldig omgaan met privacy voor negatieve publiciteit en een verlies aan vertrouwen. Aangezien bedrijven niet meer zonder informatie kunnen is het essentieel voor bedrijven om te begrijpen welke invloed privacy heeft op consumenten en waarom consumenten er voor kiezen om de verzameling van informatie (niet) te accepteren. Vandaar dat dit proefschrift antwoord probeert te geven op de volgende vraag: *Hoe worden consumenten beïnvloed door het privacy-beleid van bedrijven*? Hoewel bedrijven moeite hebben met privacy biedt de groeiende aandacht voor privacy ook kansen voor die bedrijven die in staat zijn om hun privacy-beleid af te stemmen op de wensen van de consument.

In het eerste hoofdstuk van dit proefschrift bediscussiëren we wat '*consumentenprivacy'* betekent. Hoewel privacy er oorspronkelijk over ging dat anderen niet zomaar jouw persoonlijke ruimte(s), zoals je huis, konden betreden (*fysieke privacy*), tegenwoordig is de focus verschoven naar de verzameling, opslag en het gebruik van informatie (*informatie privacy*). Voor de definitie van (informatie) privacy volgen wij recente wetgeving in de EU en de VS, waarbij het erom gaat dat consumenten zelf kunnen bepalen wat er met '*hun'* informatie gebeurt. In de context van bedrijven en consumenten definiëren we privacy daarom als *de mate waarin een consument bewust is en controle heeft over de verzameling, opslag en het gebruik van persoonlijke informatie door een bedrijf*. Dit betekent

dat zelfstandig delen van informatie geen inbreuk op privacy is en dat bedrijven alleen privacy schenden wanneer men informatie verzamelt, opslaat of gebruikt zonder consumenten te informeren of toestemming te vragen.

In hoofdstuk 2 vatten we de huidige kennis over de invloed van privacy samen door te beschrijven hoe de verzameling, opslag en gebruik van informatie door bedrijven en de mate van transparantie en controle over deze elementen, de attitudes en het gedrag van consumenten beïnvloeden. In hun privacy afweging (*privacy calculus*) zijn consumenten zich, naast de negatieve consequenties, ook bewust van de positieve consequenties van het delen van informatie. Echter is in de praktijk het gedrag van consumenten niet altijd consistent met deze privacy afweging (*privacy paradox*). Bovendien hebben de verschillende manieren van verzamelen, opslag en gebruik van informatie soms een tegenstrijdige invloed op consumenten. Bijvoorbeeld, terwijl personalisatie van producten en diensten normaal gesproken een positieve invloed heeft op klanttevredenheid, kan te gedetailleerde personalisatie ook negatieve gevoelens oproepen. Hetzelfde geldt voor transparantie, wat aan de ene kant gewaardeerd wordt door consumenten maar aan de andere kant ook juist zorgen over privacy kan activeren. Op basis van de huidige kennis identificeren we onderwerpen waar meer kennis nodig is, waar we vervolgens onderzoeksproposities voor formuleren om richting te geven aan toekomstig onderzoek.

Om de acceptatie van informatieverzameling van consumenten beter te begrijpen ontwikkelen en valideren we in het derde hoofdstuk een meetinstrument (PRICAL index) om de privacy afweging van consumenten te kunnen achterhalen. Om deze afweging beter te begrijpen kijken we zowel naar de valentie (positief én negatief) als de waarschijnlijkheid van de consequenties van informatieverzameling. Daarnaast nemen we verschillende typen consequenties (financieel, prestatie, psychologisch, sociaal, tijd, veiligheid van informatie) mee. Na validatie van de stellingen laten we in verschillende contexten zien dat ons

meetinstrument in staat is om zowel de intentie als de daadwerkelijke acceptatie van informatieverzameling beter te verklaren dan normaal gebruikte meetinstrumenten. Daarmee biedt de PRICAL index dus de mogelijkheid om beter te begrijpen waarom consumenten producten en diensten afhankelijk van de verzameling van informatie (niet) accepteren.

Omdat bedrijven nog altijd veel moeite hebben om hun privacy-beleid af te stemmen op de voorkeuren van consumenten bestuderen we in hoofdstuk 4 consumentenprivacy vanuit het perspectief van bedrijven. Met behulp van een '*choice-based conjoint*' experiment laten we zien dat de invloed van het privacy-beleid van een bedrijf op een consument verschilt per industrie. Hoewel alle elementen van het privacy-beleid (verzameling, opslag, gebruik, transparantie, controle) invloed hebben op de keuze die een consument maakt, blijkt dat met name in industrieën met gevoelige informatie de verzameling en het gebruik van informatie van belang zijn. Daarnaast hangt de invloed van het privacy-beleid van een bedrijf af van hoe men normaal gesproken binnen een industrie met privacy omgaat.

Hoewel dit proefschrift meer kennis genereert over de invloed van privacy op bedrijven en consumenten is het slechts een eerste stap. Nieuwe ontwikkelingen, zoals 'Artificial Intelligence' en het 'Internet of Things' zorgen ervoor dat bedrijven steeds beter het dagelijkse gedrag van consumenten kunnen volgen. Hoewel deze informatie potentieel enorm waardevol kan zijn is de verwachting ook dat het de zorgen over privacy ook doet toenemen. Daarom lijkt het omgaan met privacy een van de belangrijkste strategische kwesties te worden voor bedrijven.

# Chapter 9.

# Dankwoord

Na een periode van vier jaar ligt hier mijn proefschrift voor je. Toen ik vier jaar geleden begon met dit traject betrad ik een wereld waar ik eigenlijk heel weinig van wist. Een wereld van artikelen lezen, data verzamelen, publiceren, en onderzoek presenteren. Maar daarnaast ook een wereld waar ik ontzettend veel steun heb gehad van vele mensen, die ik dan ook graag wil bedanken.

Allereerst wil ik graag het Customer Insight Centre, en hierbij Jelle in het bijzonder, bedanken voor de financiering van mijn positie, maar met name voor de inspirerende bijeenkomsten en seminars. Hieraan gerelateerd wil ik ook alle bedrijven en medewerkers bedanken die mij hebben geholpen tijdens dit traject. Waar mijn proefschrift ooit begon met gesprekken bij een handvol bedrijven, werd het onderzoek enorm veel interessanter door de samenwerking met Henk-Jaap en FBTO. Bedankt voor de mogelijkheid om te bekijken hoe 'echte' klanten met hun privacy omgaan!

Verder wil ik de leden van mijn promotiecommissie, Jorg Henseler, Koert van Ittersum, en Catherine Tucker bedanken voor de tijd en moeite die ze hebben gestoken in het beoordelen van mijn proefschrift.

Daarnaast wil ik graag al mijn (ex-)collega's van de vakgroep Marketing bedanken voor de enorm prettige sfeer die er binnen de vakgroep heerst. Het feit dat je bij iedereen op de deur kan kloppen voor een inhoudelijke discussie heeft mij niet alleen enorm geholpen maar ook geïnspireerd gedurende mijn tijd als PhD. Daarnaast boden gezamenlijke lunches, en de meest uiteenlopende onderwerpen die tijdens deze lunches werden besproken, altijd de mogelijkheid om de gedachten even te verzetten.

In het bijzonder wil ik alle andere PhDs die ik tijdens mijn tijd heb mogen leren kennen naast hun hulp vooral bedanken voor hun gezelligheid. Toen ik net begon als PhD heb ik voor mijn gevoel de meer 'ervaren' PhDs eindeloos vragen gesteld over de wereld waar ik in was beland. De wekelijkse koffiemomenten, soms wat minder vaak dan anders, zorgden

altijd voor ontspanning en gaf ons de gelegenheid af en toe toch wat van de zon te genieten. Dus, Alec, Bianca, Carmen, Evert, Feng, Jacob, John, Lisette, Marit, Martine, Niels, Sander, Sebastian, Roelof, Yi-Chun, heel erg bedankt!

Dan zijn er vijf personen binnen de vakgroep die ik in het bijzonder wil bedanken. Allereerst zijn dat mijn twee promotoren: Jaap en Peter. Jullie steun heeft mij enorm geholpen en gebracht naar het niveau waar ik nu ben. Jaap, jij was altijd in staat om gedetailleerde feedback te geven die mij net weer een stap verder bracht. Peter, wanneer nodig bracht jij vaart in het onderzoek en het schrijven van artikelen, maar daarnaast wist je mij ook enorm te motiveren om het onderzoek naar een hoger niveau te brengen. Daarnaast wil ik Felix bedanken voor het feit dat hij altijd voor mij klaarstond, en ik hoop dat de rust die jij uitstraalt deels op mij is over gegaan. Dan zijn er nog twee collega's die de status van collega zijn ontgroeid. Beste Arjan en Jan, hoewel de tijd is gekomen dat we niet meer met elkaar op dezelfde plek werken hoop ik dat we nog lang vrienden mogen blijven!

Vervolgens wil ik ook graag alle andere vrienden en familie bedanken die mij de afgelopen vier jaar de nodige afleiding hebben bezorgd: het MMT, de FeFa, en de Groningen Reünie. Pa en ma, jullie interesse in mijn doen en laten heeft mij altijd gemotiveerd om het maximale eruit te halen. Wouter, Tanja en sinds kort Kay, jullie hebben mij op prachtige wijze geholpen om mijn gedachten te kunnen verzetten.

Tot slot wil ik graag de persoon bedanken die me al veel langer dan vier jaar heeft gesteund. Leonie, jouw liefde heeft me zoveel gebracht dat het moeilijk is om dit onder woorden te brengen. Wanneer het nodig is kan ik altijd bij jou terecht, en de meest fantastische reizen die we samen hebben gemaakt gaven me iedere keer weer de energie die ik nodig had. Wat ik eigenlijk wil zeggen is dat ik enorm veel van je hou!

Frank